# 信息系统等级保护安全设计技术实现与使用

范红 著



高等院校信息安全专业系列教材

# 信息系统等级保护安全设计技术实现与使用

范　红　胡志昂　金丽娜　编著

清华大学出版社
北　京

## 内 容 简 介

本书对国家标准《信息安全技术 信息系统等级保护安全设计技术要求》进行详细、深入的解读，并在此基础上给出二、三、四级系统的安全设计和实现，包括各级系统的安全功能和总体结构、实现方案和设备类型、安全计算环境子系统设计和实现、安全区域边界子系统设计和实现、安全通信网络子系统设计和实现、安全管理子系统设计和实现、审计子系统设计和实现以及典型应用子系统设计和实现，并详细介绍了各级信息系统示范环境的功能使用。书中配有各个示范环境具体操作界面的图片，使读者对示范环境有更形象生动的了解。

本书还介绍了二、三、四级安全应用平台功能符合性检验工具集使用和信息安全风险评估工具使用，主要包括：各检验工具集和风险评估工具的体系结构、功能结构、设计与实现以及使用操作演示。



**图书在版编目（CIP）数据**

信息系统等级保护安全设计技术实现与使用 / 范红，胡志昂，金丽娜编著．—北京：清华大学出版社，2010.3
高等院校信息安全专业系列教材
ISBN 978-7-302-21795-4

Ⅰ．①信…　Ⅱ．①范…　②胡…　③金…　Ⅲ．①信息系统－安全技术　Ⅳ．①TP309

中国版本图书馆 CIP 数据核字(2010)第 002438 号

**责任编辑**：张　民　李玮琪
**责任校对**：焦丽丽
**责任印制**：

**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
**社　总　机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质　量　反　馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者**：
**装 订 者**：
**经　　销**：全国新华书店
**开　　本**：185×260　　**印　　张**：14　　**字　　数**：322 千字
**版　　次**：2010 年 3 月第 1 版　　**印　　次**：2010 年 3 月第 1 次印刷
**印　　数**：1～0000
**定　　价**：0.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：-

# 前 言

信息安全等级保护是我国实现国家信息安全的基本制度，1994 年国务院 147 号令中就已规定信息系统安全实行等级保护制度，并明确指出由公安部会同有关部门制定等级保护管理办法和标准；1999 年国家发布了等级保护强制性国家标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》(以下简称 GB 17859—1999)，此后，50 多个配套标准相继发布，并已形成标准体系。这些标准的制定，为信息安全等级保护制度的实施打下了坚实的技术基础。2003 年 27 号文件则进一步明确规定国家实施信息安全等级保护制度，此后公安部等四部委联合相继发布了 66 号和 43 号文件，规定了等级保护系列政策和管理办法。

2007 年 7 月，公安部、国务院信息办等四部门联合召开全国重要信息系统等级保护定级工作会议，标志着等级保护制度在全国范围内全面展开，目前全国重要信息系统定级工作已基本完成。下一阶段的工作将对已确定安全等级的信息系统依据相关标准要求进行安全建设。此工作将涉及大量的关键技术实现难题。因此，深入开展信息系统等级保护安全体系结构及关键技术的研究，进行理论攻关、工程实践与标准制定，是即将开展的信息系统等级保护安全建设整改工作的迫切现实需要，也是国家信息安全等级保护制度长期实施所不可缺少的技术支持。本书中所介绍的信息系统等级保护安全体系结构、关键技术、等级保护模拟平台、信息系统等级保护安全建设方案以及应用案例对提高我国重要信息系统和关键基础设施的安全性有重要作用，将为各行业信息系统等级保护的安全建设提供示范与参考，也将为普遍开展的信息系统等级保护安全建设提供指导。

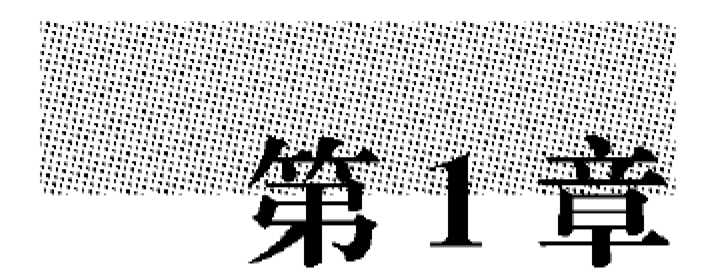
国家标准《信息安全技术　信息系统等级保护安全设计技术要求》是根据我国信息安全等级保护的实际需要，按照信息安全等级保护对信息系统安全整改的要求制定的，对信息系统等级保护安全整改阶段技术方案的设计具有指导和参考意义，本书对该标准进行了详细的解读，以帮助读者学习和理解该标准，并推进该标准的贯彻与实施。本书还从系统的安全功能和总体结构、实现方案和设备类型、安全计算环境子系统设计和实现、安全区域边界子系统设计和实现、安全通信网络子系统设计和实现、安全管理子系统设计和实现、审计子系统设计和实现以及典型应用子系统设计和实现几个方面对二、三、四级信息系统的设计和实现进行了深入的阐述，并给出了各级信息系统示范环境的功能使用

演示。本书还给出了二、三、四级安全应用平台功能符合性检验工具集和信息安全风险评估工具的设计与实现。本书从理论到实践为读者提供相关的知识。

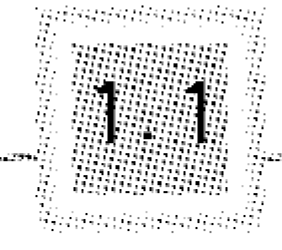
编　者

2009 年 11 月

# 目录



# 第1章 《信息系统等级保护安全设计技术要求》标准解读



## 1.1 概述

### 1.1.1 编制背景

**【标准条款】**

GB/T 24856—2009

> **引　言**
>
> 《中华人民共和国计算机信息系统安全保护条例》(国务院令第147号)明确规定我国"计算机信息系统实行安全等级保护"。依据国务院147号令要求制定发布的强制性国家标准《计算机信息系统安全保护等级划分准则》(GB 17859—1999)为计算机信息系统安全保护等级的划分奠定了技术基础。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)明确指出实行信息安全等级保护,"要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统,抓紧建立信息安全等级保护制度"。《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)确定了实施信息安全等级保护制度的原则、工作职责划分、实施要求和实施计划,明确了开展信息安全等级保护工作的基本内容、工作流程、工作方法等。
>
> 上述信息安全等级保护相关法规、政策文件、国家标准和公共安全行业标准的出台,为信息安全等级保护工作的开展提供了法律、政策、标准依据。
>
> 2007年7月,全国开展重要信息系统等级保护定级工作,标志着信息安全等级保护工作在我国全面展开。在开展信息安全等级保护定级和备案工作基础上,各单位、各部门正在按照信息安全等级保护的有关政策规定和技术标准规范,开展信息系统安全建设和加固工作,建立、健全信息安全管理制度,落实安全保护技术措施,全面贯彻落实信息安全等级保护制度。为了配合信息系统安全建设和加固工作,特制定本标准。
>
> 本标准规范了信息系统等级保护安全设计技术要求,包括第一级至第五级系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求,以及定级系统互联的设计技术要求。涉及物理安全、安全管理、安全运维等方面的要求分别参见参考文献[9]、[2]、[7]、[10][①]等。进行安全技术设计时,要根据信息系统定级情况,确定相应安全策略,采取

① 此处提到的参考文献为:[9]GB/T 21052—2007《信息安全与技术　信息系统物理安全技术要求》,[2]GB/T 20269—2006《信息安全技术　信息系统安全管理要求》,[7]GB/T 20282—2006《信息安全技术　信息系统安全工程管理要求》,[10]GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》。

相应级别的安全保护措施。

在第五章至第九章中，每一级系统安全保护环境设计比较低一级的系统安全保护环境设计所增加和增强的部分，用“黑体”表示。

**【条款解读 1】**

一、目的和意图

简要阐述标准编制的基本依据和背景情况。

二、解释和示例

国务院 1994 年 2 月 14 日发布的 147 号令《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）是我国最早提出的对计算机信息系统实行安全等级保护的法规性文件。《条例》明确规定，我国“计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。根据《条例》的要求，公安部会同有关部门，组织制定了我国第一个信息安全等级保护的强制性国家标准：GB 17859—1999《计算机信息系统安全保护等级划分准则》（注：本标准所称“信息系统”与《条例》和 GB 17859—1999 所称的“计算机信息系统”含义基本相同）。

为了推进信息安全等级保护工作的开展，公安部组织编写并于 2002 年 7 月 15 日发布了一批为 GB 17859—1999 配套并具有更好可操作性的公共安全行业标准，主要包括：GA/T 387—2002《计算机信息系统安全等级保护网络技术要求》、GA/T 388—2002《计算机信息系统安全等级保护操作系统技术要求》、GA/T 389—2002《计算机信息系统安全等级保护数据库管理系统技术要求》、GA/T 390—2002《计算机信息系统安全等级保护通用技术要求》、GA/T 391—2002《计算机信息系统安全等级保护管理要求》等。这些标准的发布对信息安全等级保护工作的开展起到了积极的推动作用。

2003 年 8 月 26 日发布的中办[2003]27 号文件（《国家信息化领导小组关于加强信息安全保障工作的意见》），确立了信息安全等级保护的基本指导思想。27 号文件明确要求在我国“实行信息安全等级保护”，指出“信息化发展的不同阶段和不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理。对涉及国家秘密的信息系统，要按照党和国家有关保密规定进行保护”。27 号文件进一步明确规定信息安全等级保护是国家信息安全基本保障制度。

根据 27 号文件关于“抓紧建立信息安全等级保护制度”的要求，公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室于 2004 年 9 月 15 日发布的《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号文件），对信息安全等级保护制度的实施作出了具体的规定，2007 年 6 月 22 日公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合修改并签发了《信息安全等级保护管理办法》（公通字[2007]43 号），对信息安全等级保护制度的具体实施工作作出了进一步的规定，并从国家安全角

度，按照信息系统的信息资源和系统服务所受到危害后对国家安全、社会秩序、公民及法人等利益产生的影响，对信息系统需要进行保护的安全等级进行了划分。

信息安全等级保护是我国信息安全的基本制度、基本政策和基本方法。国家通过信息安全等级保护管理政策和标准，从总体上规定了对信息系统实行五级安全保护。管理办法的五个安全保护等级，是从管理角度按照安全需求进行的等级划分；强制性国标GB 17859—1999及其配套系列标准中的五个安全保护等级，是按照信息安全保护能力进行的等级划分。两种等级划分是信息安全保护等级制度从不同角度的统一体现。

为了贯彻执行信息安全等级保护制度，以 GB 17859—1999 等级划分为基本依据，以上述公共安全行业标准为基础，由国家信息安全标准化技术委员会提出并组织制定了一系列信息安全国家标准，主要包括：GB/T 20269—2006《信息安全技术 信息系统安全管理要求》，GB/T 20270—2006《信息安全技术 网络基础安全技术要求》，GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》，GB/T 20272—2006《信息安全技术 操作系统安全技术要求》，GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》，GB/T 20282—2006《信息安全技术 信息系统安全工程管理要求》，GB/T 21028—2007《信息安全技术 服务器安全技术要求》，GB/T 21052—2007《信息安全技术 信息系统物理安全技术要求》，GB/T 22239—2008《信息安全技术 信息系统安全等级保护基本要求》，GB/T 22240—2008《信息安全技术 信息系统安全等级保护定级指南》等。

本标准是在这一系列信息安全等级保护相关标准的基础上，充分汲取了已经发布的一系列信息安全等级保护相关标准对于信息系统各安全要素所进行的安全等级划分的基本思想，对按照 GB/T 22240—2008 确定的每一个安全等级的定级系统的安全保护环境的设计提出了规范性的要求，对第一级至第五级定级系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术，以及系统安全互联的设计技术提出了规范性要求。本标准对于指导按照信息安全等级保护要求进行信息系统安全整改具有十分重要的意义和实际指导作用。

本标准第五章到第八章，分别对第一级系统到第四级系统安全保护环境的安全设计要求，从设计目标、设计策略、设计技术要求进行了详细描述。本标准第九章对第五级系统安全保护环境的安全设计要求，对设计目标、设计策略给出了要求，对设计技术要求的制定给出了原则性说明。本标准第十章对系统互联安全设计要求，从设计目标、设计策略、设计技术要求进行了描述。

### 1.1.2 适用范围

**【标准条款】**

GB/T 24856—2009

**1 范围**

本标准依据国家信息安全等级保护的要求，规范了信息系统等级保护安全设计技术要求。

本标准适用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构开展信息系统等级保护安全技术方案的设计和实施，也可作为信息安全职能部门进行监督、检查和指导的依据。

【条款解读 2】

一、目的和意图

界定 GB/T 20271—2006 的适用范围。

二、解释和示例

GB/T 24856—2009 的第 1 章(范围),对本标准的适用范围从涵盖内容和使用对象两个方面进行了界定:

① 按照信息安全等级保护的要求,确定信息系统等级保护安全设计的技术要求,是 GB/T 24856—2009 的内容主体,这些内容有助于使用者了解、规划和实施信息系统的安全建设,对信息系统等级保护安全整改工作具有指导和参考作用。

② 信息系统安全建设的相关人员,以及从事信息系统安全测试、管理和服务的相关人员是 GB/T 24856—2009 的主要使用对象,其他使用对象还包括任何与信息安全等级保护相关的或对信息安全等级保护感兴趣的人员。GB/T 24856—2009 对这些使用对象提出了进行信息系统等级保护安全设计的规范性要求。

### 1.1.3 规范性引用文件

【标准条款】

GB/T 24856—2009

> **2 规范性引用文件**
>
> 下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。
>
> GB 17859—1999 计算机信息系统安全保护等级划分准则

【条款解读 3】

一、目的和意图

提供 GB/T 24856—2009 正文中所引用的相关标准或规范性文件的信息。

二、解释和示例

GB/T 24856—2009 列出了 1 项强制性国家标准:

强制性国家标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》是根据 1994 年 2 月 18 日国务院发布的 147 号令的要求制定的对计算机信息系统进行安全保护等级划分的基础性标准。GB 17859—1999 按照 147 号令关于我国“计算机信息系统实行安全等级保护”的要求,以美国国防部的可信计算机系统评估准则(TCSEC,俗称“橘皮书”)为基本参考,结合我国计算机信息系统安全的实际情况,将计算机信息系统的安全划分为五个等级,并给出了每一个安全保护等级的基本要求。GB 17859—1999 尽管主要是从计算机环境对五个等级的划分准则进行描述,但是关于五个安全保护等级的划分,可以很容易就扩展到网络环境,从而为计算机网络环境的信息系统安全技术等级的划分奠定了技术基础。本标准正是按照 GB 17859—1999 的五个安全等级的划分,对组成信息系

统的计算机、网络的软硬件平台及其应用系统所涉及的通用安全技术，按照五个安全保护等级进行划分，对每一个安全保护等级应具有的安全技术要求进行描述。

### 1.1.4 术语和定义

**【标准条款】**

GB/T 24856—2009

> **3 术语和定义**
>
> GB 17859—1999 确立的以及下列术语和定义适用于本标准。

**【条款解读 4】**

一、目的和意图

描述本标准所适用的术语和定义。

二、解释和示例

本标准是以 GB 17859—1999 为基础制定的，所以 GB 17859—1999 所确立的术语应该适用于本标准。本标准同时对在本标准范围内适用的术语进行了定义。术语和定义的进一步解释，参见条款解读 5。

**【标准条款】**

GB/T 24856—2009

> **3.1 定级系统 classified system**
>
> 按照参考文献[11]①已确定安全保护等级的信息系统。定级系统分为第一级、第二级、第三级、第四级和第五级信息系统。
>
> **3.2 定级系统安全保护环境 security environment of classified system**
>
> 由安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心构成的对定级系统进行安全保护的环境。
>
> 定级系统安全保护环境包括第一级系统安全保护环境、第二级系统安全保护环境、第三级系统安全保护环境、第四级系统安全保护环境、第五级系统安全保护环境以及定级系统的安全互联。
>
> **3.3 安全计算环境 secure computing environment**
>
> 对定级系统的信息进行存储、处理及实施安全策略的相关部件。
>
> 安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。
>
> **3.4 安全区域边界 secure area boundary**
>
> 对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。
>
> 安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。

① 此处的参考文献[11]为 GB/T 22240—2008《信息系统安全等级保护定级指南》。

**3.5 安全通信网络 secure communication network**

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

**3.6 安全管理中心 security management center**

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。

第二级及第二级以上的定级系统安全保护环境需要设置安全管理中心，称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

**3.7 跨定级系统安全管理中心 security management center for cross classified system**

跨定级系统安全管理中心是对相同或不同等级的定级系统之间互联的安全策略及安全互联部件上的安全机制实施统一管理的平台。

**3.8 定级系统互联 classified system interconnection**

通过安全互联部件和跨定级系统安全管理中心实现的相同或不同等级的定级系统安全保护环境之间的安全连接。

**【条款解读 5】**

一、目的和意图

对本标准适用的术语进行定义。

二、解释和示例

GB/T 24856—2009 的第 3 章(术语和定义)，对本标准所适用的术语进行了定义。本标准是以 GB 17859—1999 为基础制定的，所以 GB 17859—1999 所确立的术语应该适用于本标准。除了 GB 17859—1999 所定义的相关术语适用于本标准外，本标准对正文中出现的以下术语进行了定义：

① 定级系统，是指按照《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240—2008)已确定安全保护等级的信息系统。定级系统安全保护环境是指，由安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心构成的对定级系统进行安全保护的环境。

② 定级系统安全保护环境，是指按等级保护要求对定级系统进行安全保护的环境，由安全计算环境、安全区域边界、安全通信网络和安全管理中心(二级以上设安全管理中心)构成，按照安全保护能力可划分为第一级安全保护环境、第二级安全保护环境、第三级安全保护环境、第四级安全保护环境和第五级安全保护环境。

③ 安全计算环境，是指对定级系统的信息进行存储、处理及实施安全保护的相关部件。计算环境由定级系统中完成信息存储与处理的计算机系统硬件和系统软件以及外部设备及其连接部件组成。安全计算环境是具有一定安全保护能力的计算环境，按照安全保护能力可划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

④ 安全区域边界，是指对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全保护的相关部件。安全区域边界是对安全计算环境以及进出安全计算环境的信息具有一定安全保护能力的区域边界，按照安全保护能力可划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域

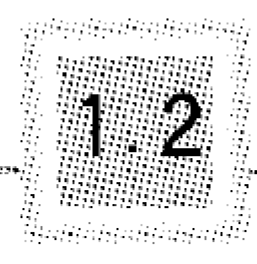
边界和第五级安全区域边界。

⑤ 安全通信网络，是指对定级系统安全计算环境之间进行信息传输及实施安全保护的部件。安全通信网络是具有一定安全保护能力的通信网络，按照安全保护能力可划分为第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

⑥ 安全管理中心，是指对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。第二级及其以上的安全保护环境通常需要设置安全管理中心，分别称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

⑦ 跨定级系统安全管理中心，是指对相同或不同等级的定级系统之间安全互联的安全策略及安全互联部件上的安全机制实施统一管理的平台。

⑧ 定级系统互联，是指为相同或不同等级的定级系统安全保护环境之间实施安全互联和安全管理的部件。定级系统安全互联由安全互联部件和跨定级系统安全管理中心组成。安全互联部件通常由具有相应安全功能的安全网关构成。



## 1.2 信息系统等级保护安全设计概述

**【标准条款】**

GB/T 24856—2009

**4 信息系统等级保护安全技术设计概述**

信息系统等级保护安全技术设计包括各级系统安全保护环境的设计及其安全互联的设计，如图 1

第一级系统安全保护环境
第一级安全计算环境
第一级安全区域边界
第一级安全通信网络

第二级系统安全保护环境
第二级安全计算环境
第二级安全区域边界
第二级安全通信网络
第二级安全管理中心

第三级系统安全保护环境
第三级安全计算环境
第三级安全区域边界
第三级安全通信网络
第三级安全管理中心

第四级系统安全保护环境
第四级安全计算环境
第四级安全区域边界
第四级安全通信网络
第四级安全管理中心

第五级系统安全保护环境
第五级安全计算环境
第五级安全区域边界
第五级安全通信网络
第五级安全管理中心

定级系统互联
安全互联部件
跨定级系统安全管理中心

**图 1 信息系统等级保护安全技术设计框架**

> 所示。各级系统安全保护环境由相应级别的安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心组成。定级系统互联由安全互联部件和跨定级系统安全管理中心组成。
>
> 本标准以下章节,对图1各个部分提出了相应的设计技术要求(第五级信息安全保护环境的设计要求除外)。附录A给出了访问控制机制设计,附录B给出了第三级系统安全保护环境设计示例。

**【条款解读6】**

一、目的和意图

对信息系统等级保护安全设计进行概要描述。

二、解释和示例

GB/T 24856—2009的第4章(信息系统等级保护安全设计概述),概要描述了按照信息系统安全等级保护的要求进行安全信息系统的安全设计。

本章以图示的形式给出了信息系统等级保护安全技术设计框架。按图1所示,一个典型的多级安全信息系统由第一级系统安全保护环境、第二级系统安全保护环境、第三级系统安全保护环境、第四级系统安全保护环境、第五级系统安全保护环境以及安全定级系统互联等部分组成。其中每一级系统安全保护环境分别由具有符合第一级安全要求的安全计算环境、安全区域边界、安全通信网络和安全管理中心组成。安全系统互联则由系统安全互联部件和跨系统安全管理中心组成。

以下是信息系统安全等级保护设计的示例。通过该示例将把标准中图1所示的信息系统等级保护安全技术设计与典型信息系统的安全保护设计相联系。

图1-1是典型信息系统安全保护总体结构的示意图,是当前我国大部分部委信息系统的实际结构的抽象表示。

按图1-1所示,一个典型的信息系统安全保护总体结构,由总部安全信息系统、省级安全信息系统和地级安全信息系统(必要时可延伸至县级安全信息系统)等三层的安全信息系统组成。各层安全信息系统相对独立,可以看作是独立的信息系统;各层安全信息系统又通过内网安全通信网络相互连接,可以看作是一个综合的安全信息系统。其中,总部和省级层数据中心安全计算环境、各层业务处理计算环境、各层内部终端安全计算环境、各层外部安全计算环境对应于标准图1中的安全计算环境;各层安全计算环境相应的安全区域边界对应于标准图1中的安全区域边界(各层终端计算环境的安全区域边界没有显式表示出来);各层内、外网安全通信网络对应于标准图1中的安全通信网络。

各层安全信息系统由各层业务处理安全计算环境及其安全区域边界、各层外部终端安全计算环境、各层内部终端安全计算环境、各层数据中心安全计算环境(地级除外)、各层安全管理中心以及各层内网安全通信网络和各层外网安全通信网络等部分组成。标准中所称定级系统,分别由各层业务处理安全计算环境中的各个业务处理安全计算环境与相应各层内、外部终端安全计算环境及实现其互联的各层内、外部安全通信网络组成的系统,其安全保护等级由系统中所包含的安全计算环境的最高安全等级确定。

根据业务数据和业务处理的安全要求,总部安全信息系统中,作为数据集中存储和处理的总部数据中心安全计算环境及其安全区域边界一般需要进行四级或三级安全保护,

图 1-1 典型信息系统安全保护总体结构

总部业务处理安全计算环境及其区域边界一般需要进行三级或二级安全保护，总部内、外部终端安全计算环境一般需要进行二级或一级安全保护，作为连接总部各安全计算环境的总部内、外网安全通信网络，通常根据其所传输数据的安全保护需求来确定其应具有的安全保护等级；省级安全信息系统中，作为数据集中存储和处理的省级数据中心安全计算环境及其安全区域边界一般需要进行三级安全保护，省级业务处理安全计算环境及其区域边界一般需要进行二级或三级安全保护，省级内、外部终端安全计算环境一般需要进行一级或二级全保护，作为连接各省级各安全计算环境的省级内、外网安全通信网络，通常根据其所传输数据的安全保护需求来确定其应具有的安全保护等级；地级安全信息系统中，地级业务处理安全计算环境及其区域边界一般需要进行二级安全保护，地级内、外部

终端安全计算环境一般需要进行一级或二级全保护，作为连接地级各安全计算环境的地级内、外网安全通信网络，通常根据其所传输数据的安全保护需求来确定其应具有的安全保护等级。

需要进一步说明的是，按照上述结构，一个定级系统可以包括一个或多个不同安全保护等级的安全计算环境及其安全区域边界，以及根据这些安全计算环境之间所传输的数据需求确定的内、外部安全通信网络。另外，由于多个定级系统往往运行于同一个物理环境之上，对于安全计算环境而言，一般只能按照较高等级来进行安全机制配置，而对于安全通信网络则可以采用建立虚拟专用网等方式来实现不同安全等级的安全保护。

图 1-1 中分别给出了跨系统安全互联各层安全信息系统的安全互联，包括安全互联部件和跨系统互联安全管理中心。在具体实现上，可以在各层设置安全互联部件和跨系统互联安全管理中心，实现各层安全信息系统范围内的跨系统安全互联，也可以全系统设置统一的安全互联部件和全系统跨系统互联安全管理中心，实现整个安全信息系统范围的跨系统安全互联。

连接不同等级安全计算环境的安全通信网络，一般应具有与较低安全等级的安全计算环境相同的安全等级。因为无论是从较高等级的安全计算环境向较低等级的安全计算环境传输数据，还是从较低等级的安全计算环境向较高等级的安全计算环境传输数据，数据在传输过程中的安全保护需求，都可以作为较低等级安全计算环境安全保护需求的延伸。

## 1.3 第一级信息系统安全保护环境设计

**【标准条款】**

GB/T 24856—2009

| |
|---|
| **5 第一级系统安全保护环境设计** |

**【条款解读 7】**

一、目的和意图

描述第一级信息系统安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 5 章(第一级系统安全保护环境设计)，从设计目标、设计策略和设计技术要求等方面，对第一级信息系统安全保护环境的安全设计要求进行描述。

有关第一级信息系统安全保护环境的安全设计要求的进一步解释，参见条款解读 8、条款解读 9 和条款解读 10。

### 1.3.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **5.1 设计目标**
>
> 第一级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第一级系统的安全保护要求，实现定级系统的自主访问控制，使系统用户对其所属客体具有自我保护的能力。

**【条款解读 8】**

一、目的和意图

描述第一级信息系统安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 5.1(设计目标)，对第一级信息系统安全保护环境的安全设计目标进行了描述。强调第一级信息系统安全保护环境的安全设计是对 GB 17859—1999 用户自主保护级安全保护要求的具体实现。安全设计目标是：达到提供用户对其所属客体进行自主保护的水平。

第一级信息系统安全保护环境的安全设计目标，应根据信息安全等级保护有关政策法规(如公通字[2004]66 号文件和公通字[2007]43 号文件等)对第一级信息系统安全要求的描述，按照风险分析的方法所确定的目标信息系统的安全需求，以及信息安全等级保护相关标准对适用于第一级信息系统的安全要素和安全产品的具体要求，综合分析进行确定。

### 1.3.2 安全设计策略

**【标准条款】**

GB/T 24856—2009

> **5.2 设计策略**
>
> 第一级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.1 中相关要求，以身份鉴别为基础，提供用户和(或)用户组对文件及数据库表的自主访问控制，以实现用户与数据的隔离，使用户具备自主安全保护的能力；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段提供数据和系统的完整性保护。
>
> 第一级系统安全保护环境的设计通过第一级的安全计算环境、安全区域边界以及安全通信网络的设计加以实现。

**【条款解读 9】**

一、目的和意图

描述第一级信息系统安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 5.2(设计策略),强调第一级信息系统安全保护环境的安全设计应遵循 GB 17859—1999 的 4.1 的相关要求,以身份鉴别、访问控制和传输数据完整性保护为基本的安全保护机制;具体通过对安全计算环境、安全区域边界以及安全通信网络的安全设计,实现第一级信息系统安全保护环境的安全设计目标。

在第一级信息系统安全保护环境的安全设计中,安全策略应是对实现第一级信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

## 1.3.3 安全设计技术要求

**【标准条款】**

GB/T 24856—2009

| |
|---|
| **5.3 设计技术要求** |

**【条款解读 10】**

一、目的和意图

描述第一级信息系统安全保护环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 5.3(设计技术要求),从安全计算环境安全设计、安全区域边界安全设计和安全通信网络安全设计等方面,对第一级信息系统安全保护环境的安全设计技术要求进行描述。

计算环境和通信网络是信息系统不可缺少的组成部分。第一级安全计算环境,是按照所确定的第一级信息系统安全保护环境的安全设计目标和安全设计策略对安全计算环境的安全要求,在计算环境所实现的计算功能的基础上,附加实现相应安全保护功能的对计算环境进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全计算环境;第一级安全通信网络,是按照所确定的第一级信息系统安全保护环境的安全设计目标和安全设计策略对通信网络的安全要求,在通信网络所实现的通信功能的基础上,附加实现相应安全保护功能的对通信网络功能进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全通信网络。

安全区域边界是专为在安全计算环境的边界进行安全保护而设置的。第一级安全区域边界是按照确定的第一级信息系统安全保护环境的安全设计目标和安全设计策略对区域边界的安全要求,采用具有相应安全保护能力的安全技术和安全产品构成的区域边界。

安全计算环境、安全区域边界和安全通信网络三者中的安全机制协同运行,共同实现第一级信息系统的安全保护目标。

有关第一级信息系统安全保护环境的安全设计技术要求的进一步解释,参见条款解读 11、条款解读 12 和条款解读 13。

**【标准条款】**

GB/T 24856—2009

> **5.3.1 安全计算环境设计技术要求**
>
> 第一级安全计算环境从以下方面进行安全设计：
>
> a) 用户身份鉴别
>
> 应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份；在每次用户登录系统时，采用口令鉴别机制进行用户身份鉴别，并对口令数据进行保护。
>
> b) 自主访问控制
>
> 应在安全策略控制范围内，使用户/用户组对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户/用户组。访问控制主体的粒度为用户/用户组级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。
>
> c) 用户数据完整性保护
>
> 可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。
>
> d) 恶意代码防范
>
> 应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

**【条款解读 11】**

一、目的和意图

描述第一级信息系统安全计算环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 5.3.1(安全计算环境设计技术要求)，从用户身份鉴别、自主访问控制、用户数据完整性保护、恶意代码防范等方面，对第一级信息系统安全计算环境的安全设计技术要求进行描述。

第一级信息系统的安全计算环境，要求对计算环境进行最基本的安全保护，主要是通过选择具有第一级安全的操作系统和数据库管理系统实现对安全计算环境的安全保护。第一级安全的操作系统应符合 GB/T 20272—2006《信息安全技术 操作系统安全技术要求》的 4.1 关于第一级安全操作系统的基本要求；第一级安全的数据库管理系统应符合 GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》的 5.1 关于第一级安全操作系统的基本要求。在操作系统和数据库管理系统中应采用基本的用户身份鉴别、粗粒度的自主访问控制和用户数据的完整性保护进行安全保护，以及通过配置防病毒软件，实现对恶意代码的防范，使系统能正常运行。

**【标准条款】**

GB/T 24856—2009

> **5.3.2 安全区域边界设计技术要求**
>
> 第一级安全区域边界从以下方面进行安全设计：

a) 区域边界包过滤

可根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

b) 区域边界恶意代码防范

可在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。

**【条款解读 12】**

一、目的和意图

描述第一级信息系统安全区域边界设计的安全技术要求。

二、解释和示例

GB/T 24856—2009 的 5.3.2(安全区域边界设计技术要求)，从区域边界包过滤、区域边界恶意代码防范等方面，对第一级信息系统安全区域边界设计的安全技术要求进行描述。

第一级信息系统的安全区域边界，通过安全区域边界的安全设计，对来自外部的对安全计算环境的攻击进行基本的安全防护，具体做法是，通过选择和配置符合第一级安全要求的区域边界包过滤和区域边界恶意代码防范的安全机制和(或)产品进行边界防护，以对抗来自外部的攻击。

**【标准条款】**

GB/T 24856—2009

**5.3.3 安全通信网络设计技术要求**

a) 通信网络数据传输完整性保护

可采用常规校验机制，检验通信网络数据传输的完整性，并能发现其完整性被破坏。

**【条款解读 13】**

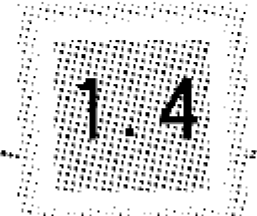
一、目的和意图

描述第一级信息系统安全通信网络的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 5.3.3(安全通信网络设计技术要求)，提出安全通信网络安全设计的基本技术要求，主要是采用各种常规校验机制检验通信网络传输数据的完整性，发现其完整性被破坏的情况。

第一级信息系统的安全通信网络，通过安全通信网络的安全设计，对通信网络的安全运行和通信网络所传输的数据进行基本的安全保护，具体做法是通过采用各种常规的符合第一级安全要求的完整性校验技术和机制，发现通过通信网络传输的用户数据其完整性被破坏的情况。



# 1.4 第二级信息系统安全保护环境设计

**【标准条款】**

GB/T 24856—2009

> **6 第二级系统安全保护环境设计**

**【条款解读 14】**

一、目的和意图

描述第二级信息系统安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 6 章，第二级系统安全保护环境设计，从设计目标、设计策略和设计技术要求等方面，对第二级信息系统安全保护环境的安全设计要求进行了描述。

有关第二级信息系统安全保护环境的安全设计要求的进一步解释，参见条款解读 15～条款解读 17。

## 1.4.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **6.1 设计目标**
>
> 第二级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第二级系统的安全保护要求，在第一级系统安全保护环境的基础上，增加系统安全审计、客体重用等安全功能，并实施以用户为基本粒度的自主访问控制，使系统具有更强的自主安全保护能力。

**【条款解读 15】**

一、目的和意图

描述第二级信息系统安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 6.1(设计目标)，对第二级信息系统安全保护环境的安全设计目标进行了描述。强调第二级信息系统安全保护环境的安全设计是对 GB 17859—1999 系统审计保护级安全保护要求的具体实现，是在第一级系统安全保护环境所设置的安全机制的基础上，通过增加和增强安全机制，从系统角度对用户所属客体进行安全保护。安全设计目标是达到使系统具有更强的自主安全保护能力的水平。

第二级信息系统安全保护环境的安全设计目标，应根据信息安全等级保护的有关政策法规(如公通字[2004]66 号文件和公通字[2007]43 号文件等)对第二级信息系统安全

要求的描述，按照风险分析方法所确定的目标信息系统的安全需求，以及信息安全等级保护相关标准对适用于第二级信息系统的安全要素和安全产品的具体要求，综合分析进行确定。

### 1.4.2 安全设计策略

**【标准条款】**

GB/T 24856—2009

> **6.2 设计策略**
>
> 第二级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.2 中相关要求，以身份鉴别为基础，提供单个用户和(或)用户组对共享文件、数据库表等的自主访问控制；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段，同时通过增加系统安全审计、客体安全重用等功能，使用户对自己的行为负责，提供用户数据保密性和完整性保护，以增强系统的安全保护能力。
>
> 第二级系统安全保护环境的设计通过第二级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

**【条款解读 16】**

一、目的和意图

描述第二级信息系统安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 6.2(设计策略)，强调第二级信息系统安全保护环境的安全设计应遵循 GB 17859—1999 的 4.2 的相关要求，在第一级安全设计的基础上，增强自主访问控制、增加安全审计和客体安全重用等安全机制，实现数据存储和传输的完整性和保密性保护；具体通过对安全计算环境、安全区域边界、安全通信网络的安全设计，以及以安全管理中心的设计实现第二级信息系统安全保护环境的安全设计目标。

在第二级信息系统安全保护环境的安全设计中，安全策略应是对实现第二级信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

### 1.4.3 安全设计技术要求

**【标准条款】**

GB/T 24856—2009

> **6.3 设计技术要求**

**【条款解读 17】**

一、目的和意图

描述第二级信息系统安全保护环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 6.3(设计技术要求),从安全计算环境安全设计、安全区域边界安全设计、安全通信网络安全设计和安全管理中心设计等方面,对第二级信息系统安全保护环境的安全设计技术要求进行描述。

计算环境和通信网络是信息系统不可缺少的组成部分。第二级安全计算环境,是按照所确定的第二级信息系统安全保护环境的安全设计目标和安全设计策略对安全计算环境的安全要求,在计算环境所实现的计算功能的基础上,附加实现相应安全保护功能的对计算环境进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全计算环境;第二级安全通信网络,是按照所确定的第二级信息系统安全保护环境的安全设计目标和安全设计策略对通信网络的安全要求,在通信网络所实现的通信功能的基础上,附加实现相应安全保护功能的对通信网络功能进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全通信网络。

安全区域边界是专为在安全计算环境的边界进行安全保护而设置的。第二级安全区域边界是按照确定的第二级信息系统安全保护环境的安全设计目标和安全设计策略对区域边界的安全要求,采用具有相应安全保护能力的安全技术和安全产品构成的区域边界。

安全管理中心是专对信息系统安全保护环境进行集中管理设置的。第二级信息系统安全保护环境的安全管理中心,统一管理和控制系统中的安全审计机制,汇集、存储并分析来自各安全机制和产品的审计信息。

安全计算环境、安全区域边界和安全通信网络三者中的安全机制,以及安全管理中心协同运行,共同实现第二级信息系统的安全保护目标。

第二级信息系统安全保护环境的安全设计应特别注重对系统安全审计的设计。安全审计机制贯穿于整个安全系统的设计之中,使之成为一个整体。安全审计虽然不是一种对攻击和破坏直接进行对抗的安全技术,但是完备的安全审计系统和完整的具有良好可用性的审计日志,能够有效地提供安全事件的可查性。安全审计与严格的身份鉴别相结合,可将安全事件落实到具体的用户,从而具有很强的威慑作用。

第二级信息系统安全保护环境的安全设计,应注意在安全计算环境、安全区域边界和安全通信网络中,将安全审计和恶意代码防范等安全机制的设置统一进行考虑,使之成为一个实现全系统安全保护的整体。

有关第二级信息系统安全保护环境的安全设计技术要求的进一步解释,参见条款解读 18 至条款解读 21。

**【标准条款】**

GB/T 24856—2009

**6.3.1 安全计算环境设计技术要求**

第二级安全计算环境从以下方面进行安全设计:

a) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时,采用用户名和用户标识符标识用户身份,并确保在系统整个生存周期用户标识的唯一性;在每次用户登录系统时,采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别,并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

c) 系统安全审计

应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。

d) 用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

e) 用户数据保密性保护

可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

f) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

g) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

**【条款解读 18】**

一、目的和意图

描述第二级信息系统安全计算环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 6.3.1(安全计算环境设计技术要求)，从用户身份鉴别、自主访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、恶意代码防范等方面，对第二级信息系统安全计算环境的安全设计技术要求进行描述。

第二级信息系统的安全计算环境，要求对计算环境进行一定程度的安全保护，选择具有第二级安全的操作系统和数据库管理系统实现对安全计算环境的安全保护。第二级安全的操作系统应符合 GB/T 20272—2006《信息安全技术 操作系统安全技术要求》的 4.2 关于第二级安全操作系统的基本要求；第二级安全的数据库管理系统应符合 GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》的 5.2 关于第二级安全数据库管理系统的基本要求。在操作系统和数据库管理系统中，应采用增强管理的用户身份鉴别(包括在整个系统生存周期用户标识的唯一性和对口令鉴别信息在长度和字符选择方面的增强要求)，中粒度的自主访问控制和较强安全性的用户数据的完整性保护，以及包括客体安全重用在内的用户数据保密性保护，并通过较完整的恶意代码的防范措施，及时进行产品升级和数据更新，来对抗计算机病毒的侵袭，确保系统正常运行。

第二级信息系统的安全计算环境的安全审计机制是分散在安全操作系统和安全数据

库管理系统以及其他安全机制和安全产品之中的，在进行安全计算机环境的安全机制设置和安全产品选择时，应注意其中的审计机制与安全管理中心的安全审计集中管理有一致的标准接口。

安全区域边界的恶意代码防范应与安全计算环境的恶意代码防范整体考虑，通过选取相应的防病毒产品，共同实现防恶意代码侵犯的目标。

**【标准条款】**

GB/T 24856—2009

> **6.3.2 安全区域边界设计技术要求**
>
> 第二级安全区域边界从以下方面进行安全设计：
>
> a) 区域边界包过滤
>
> 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。
>
> b) 区域边界安全审计
>
> 应在安全区域边界设置审计机制，并由安全管理中心统一管理。
>
> c) 区域边界恶意代码防范
>
> 应在安全区域边界设置防恶意代码网关，由安全管理中心管理。
>
> d) 区域边界完整性保护
>
> 应在区域边界设置探测器，探测非法外联等行为，并及时报告安全管理中心。

**【条款解读 19】**

一、目的和意图

描述第二级信息系统安全区域边界设计的安全技术要求。

二、解释和示例

GB/T 24856—2009 的 6.3.2(安全区域边界设计技术要求)，从区域边界包过滤、区域边界安全审计、区域边界恶意代码防范以及区域边界完整性保护等方面，对第二级信息系统安全区域边界设计的安全技术要求进行描述。

第二级信息系统的安全区域边界，要求通过安全区域边界的安全设计，对来自外部的对安全计算环境的攻击进行一般性的安全防护，具体做法是，在第一级安全区域边界安全设计的基础上，通过选择和配置具有符合第二级安全要求的区域边界包过滤、区域边界恶意代码防范和区域边界完整性保护等安全机制和(或)产品，进行边界防护，并通过设置安全审计机制，增强安全保护能力，以对抗来自外部的攻击。

第二级信息系统的安全区域边界的安全审计机制是分散在区域边界包过滤和区域边界完整性保护等安全机制和产品之中的，在进行安全区域边界的安全机制设置和安全产品选择时，应注意其中的审计机制与安全管理中心的安全审计集中管理有一致的标准接口。

安全区域边界的恶意代码防范应从安全计算环境的恶意代码防范整体考虑，通过选取相应的防病毒产品，共同实现防恶意代码侵犯的目标。

**【标准条款】**

GB/T 24856—2009

> **6.3.3 安全通信网络设计技术要求**
>
> 第二级安全通信网络从以下方面进行安全设计：
>
> a) 通信网络安全审计
>
> 应在安全通信网络设置审计机制，由安全管理中心管理。
>
> b) 通信网络数据传输完整性保护
>
> 可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。
>
> c) 通信网络数据传输保密性保护
>
> 可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

**【条款解读 20】**

一、目的和意图

描述第二级信息系统安全通信网络的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 6.3.3(安全通信网络设计技术要求)，从通信网络安全审计、通信网络数据传输完整性保护、通信网络数据传输保密性保护等方面，对第二级信息系统安全通信网络的安全设计技术要求进行描述。

第二级信息系统的安全通信网络，通过安全通信网络的安全设计，对通信网络的安全运行和通信网络所传输的数据进行一般性的安全保护，具体做法是，在第一级安全通信网络安全设计的基础上，通过选择和配置具有符合第二级安全要求的通信网络安全审计、通信网络数据传输完整性和保密性保护的安全机制和(或)产品，实现通信网络的安全保护。

第二级信息系统的安全通信网络的安全审计机制是分散在通信网络数据传输完整性保护和通信网络数据传输保密性保护等安全机制和产品之中的，在进行安全通信网络的安全机制设置和安全产品选择时，应注意其中的审计机制与安全管理中心的安全审计集中管理有一致的标准接口。

**【标准条款】**

GB/T 24856—2009

> **6.3.4 安全管理中心设计技术要求**
>
> 6.3.4.1 系统管理
>
> 可通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份和授权管理、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。
>
> 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

> 6.3.4.2 审计管理
>
> 可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。
>
> 应对安全审计员进行身份鉴别，并只允许其通过特定的命令或操作界面进行安全审计操作。

**【条款解读 21】**

一、目的和意图

描述第二级信息系统安全管理中心设计的技术要求。

二、解释和示例

GB/T 24856—2009 的 6.3.4(安全管理中心设计技术要求)，从系统管理和审计管理等方面，对第二级信息系统安全管理中心设计技术要求进行描述。

第二级信息系统的安全管理中心的设计，是在信息系统原有系统管理的基础上，通过对分布在安全计算环境、安全区域边界和安全通信网络等各组成部分中的安全审计的集中管理，增强信息系统各安全机制的整体安全保护能力。

第二级信息系统安全管理中心安全审计管理，是对分散在安全计算环境、安全区域边界和安全通信网络中的各安全审计机制实施集中管理的机制。在进行安全审计管理的设计或选择相应的安全审计集中管理产品时，应注意其与分散在安全计算环境、安全区域边界和安全通信网络的各安全机制具有一致的标准接口。

## 1.5 第三级信息系统安全保护环境设计

**【标准条款】**

GB/T 24856—2009

> 7 第三级系统安全保护环境设计

**【条款解读 22】**

一、目的和意图

描述第三级信息系统安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 7 章(第三级系统安全保护环境设计)，从设计目标、设计策略和设计技术要求等各方面，对第三级信息系统的安全保护环境的安全设计要求进行描述。

有关第三级系统安全保护环境的安全设计要求的进一步解释，参见条款解读 23～条款解读 25。

### 1.5.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **7.1 设计目标**
>
> 第三级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第三级系统的安全保护要求，在第二级系统安全保护环境的基础上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使系统具有在统一安全策略管控下，保护敏感资源的能力。

**【条款解读 23】**

一、目的和意图

描述第三级信息系统安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 7.1(设计目标)，对第三级信息系统安全保护环境的安全设计目标进行了描述。强调第三级信息系统安全保护环境的安全设计是对 GB 17859—1999 系统审计保护级安全保护要求的具体实现，是在第二级信息系统安全保护环境所提供的安全机制的基础上，通过增加标记与强制访问控制等安全机制，使系统在安全管理中心统一的安全策略管控下，提供对重要信息系统的安全运行和数据进行安全保护的能力。安全设计目标是达到整个信息系统的安全保护能力，并能够抵御各种常见攻击的水平。

第三级信息系统安全保护环境的安全设计目标，应根据信息安全等级保护的有关政策法规(如公通字[2004]66 号文件和公通字[2007]43 号文件等)对第三级信息系统安全要求的描述，按照风险分析的方法所确定的目标信息系统的安全需求，以及信息安全等级保护相关标准对适用于第三级信息系统的安全要素和安全产品的具体要求，综合分析进行确定。

### 1.5.2 安全设计策略

**【标准条款】**

GB/T 24856—2009

> **7.2 设计策略**
>
> 第三级系统安全保护环境的设计策略是：在第二级系统安全保护环境的基础上，遵循 GB 17859—1999 的 4.3 中相关要求，构造非形式化的安全策略模型，对主、客体进行安全标记，表明主、客体的级别分类和非级别分类的组合，以此为基础，按照强制访问控制规则实现对主体及其客体的访问控制。
>
> 第三级系统安全保护环境的设计通过第三级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

【条款解读 24】

一、目的和意图

描述第三级信息系统安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 7.2(设计策略),强调第三级信息系统安全保护环境的安全设计应遵循 GB 17859—1999 的 4.3 的相关要求,在第二级安全设计的基础上,通过构建非形式化的安全策略模型,增加标记和强制访问控制等安全机制,使系统的安全性有明显的提升,并对数据存储和传输保护等其他安全功能的安全性有一个较大的提高,使之与强制访问控制相匹配;具体做法是通过对安全计算环境、安全区域边界、安全通信网络的安全设计,以及以安全管理中心的设计,实现第三级信息系统安全保护环境的安全设计目标。

在第三级信息系统安全保护环境的安全设计中,安全策略应是对实现第三级信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

## 1.5.3 安全设计技术要求

【标准条款】

GB/T 24856—2009

| |
|---|
| **7.3 设计技术要求** |

【条款解读 25】

一、目的和意图

描述第三级信息系统安全保护环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 7.3(设计技术要求),从安全计算环境安全设计、安全区域边界安全设计、安全通信网络安全设计和安全管理中心设计等方面,对第三级信息系统安全保护环境的安全设计技术要求进行描述。

计算环境和通信网络是信息系统不可缺少的组成部分。第三级安全计算环境,是按照所确定的第三级信息系统安全保护环境的安全设计目标和安全设计策略对安全计算环境的安全要求,在计算环境所实现的计算功能的基础上,附加实现相应安全保护功能的对计算环境进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全计算环境;第三级安全通信网络,是按照所确定的第三级信息系统安全保护环境的安全设计目标和安全设计策略对通信网络的安全要求,在通信网络所实现的通信功能的基础上,附加实现相应安全保护功能的对通信网络功能进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全通信网络。

安全区域边界是专为在安全计算环境的边界进行安全保护而设置的。第三级安全区域边界是按照确定的第三级信息系统安全保护环境的安全设计目标和安全设计策略对区域边界的安全要求,采用具有相应安全保护能力的安全技术和安全产品构成的区域边界。

安全管理中心是专为对信息系统安全保护环境进行集中管理设置的。第三级信息系统安全保护环境的安全管理中心统一管理和控制系统中需要进行集中管理的安全策略和分布式安全机制，包括需要进行的主客体统一标记、主体授权和强制访问控制，以及分散在系统各组成部分的需要进行集中控制和管理的各种安全机制的管理。

安全计算环境、安全区域边界和安全通信网络三者中的安全机制，在安全管理中心的管理之下，实施统一的安全策略，协同运行，共同实现第三级信息系统的安全保护目标。

第三级信息系统的安全保护环境，应对信息系统进行较高程度的安全保护，在第二级安全保护环境安全设计的基础上，通过在安全计算环境和安全区域边界实施强制访问控制，使安全计算环境的抗攻击能力得到较大提高，同时要求在用户身份鉴别、用户数据的完整性保护和保密性保护等方面，均达到与强制访问控制相匹配的水平。比如，采用较完整的密码体系，实现用户身份鉴别、签名、验证、抗抵赖，实现用户数据的保密性、完整性保护，以及程序可信执行保护等，并通过较完整的安全管理中心实现对整个信息系统安全保护环境安全策略的统一管理。

有关第三级信息系统安全保护环境安全设计技术要求的进一步解释，参见条款解读26～条款解读29。

**【标准条款】**

GB/T 24856—2009

**7.3.1 安全计算环境设计技术要求**

第三级安全计算环境从以下方面进行安全设计：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e）用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f）用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

g）客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h）程序可信执行保护

可构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

**【条款解读 26】**

一、目的和意图

描述第三级信息系统安全计算环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 7.3.1（安全计算环境设计技术要求），从用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、程序可信执行保护等方面，对第三级信息系统安全计算环境的安全设计技术要求进行描述。

第三级信息系统的安全计算环境要求对计算环境进行较高程度的安全保护，选择具有第三级安全的操作系统和数据库管理系统实现对安全计算环境的安全保护。第三级安全的操作系统应符合 GB/T 20272—2006《信息安全技术 操作系统安全技术要求》的 4.3 关于第三级安全操作系统的基本要求；第三级安全的数据库管理系统应符合 GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》的 5.3 关于第三级安全数据库管理系统的基本要求。在第二级安全设计的基础上，在操作系统和数据库管理系统中，通过增加标记和强制访问控制的安全机制，使系统的抗攻击能力提高到一个较高的水平，同时要求在用户身份鉴别和用户数据的完整性保护和保密性保护等方面，均应达到与强制访问控制相匹配的水平。

标记和强制访问控制，是第三级信息系统安全计算环境比第二级信息系统安全计算环境对安全性有明显增强的新增安全功能。在本标准所涉及的安全计算环境中，标记和强制访问控制一般是在安全操作系统和安全数据库管理系统中实现的。由于美国目前还禁止具有强制访问控制功能的 B1 级以上操作系统对我国出口，我国市场上当前能够见到的都是在 C2 级操作系统和数据库管理系统的基础上，以增加标记和强制访问控制为中心进行操作系统的安全加固，一般可以达到第三级安全操作系统的要求。数据库管理系统的安全加固由于大型数据库产品的规模和复杂性，使得其难度较大。不过有一些国产数据库产品声称已经达到 B1 级或 B2 级的要求，只是市场的广泛认可还需要有一个过

程(国外也有对操作系统和数据库管理系统进行安全加固的产品,如 AutoSecure ACWNT 和 Trusted Oracle 等)。

操作系统和数据库管理系统中的标记和强制访问控制机制是以对主体和客体的标记为基础,以相应的强制访问控制规则为基本依据来确定主体对客体的访问权限的。其主体标记都是以用户作为基本的标记对象,而客体则有所不同。操作系统一般以文件作为客体,数据库管理系统一般以库表作为客体。虽然通常数据库的库表是建立在操作系统文件的基础之上的,但是两者的访问控制机制却是不能相互替代的,因为它们各自只能在自己所控制的范围起作用。对于在组成安全计算环境的各个计算机系统上实施相同安全策略的访问控制机制的情况,需要由安全管理中心对安全策略进行统一管理,并进行统一的主、客体安全标记。而跨定级系统实施统一安全策略的访问开展,则需要由跨定级系统安全管理中心来进行统一安全策略管理,并统一进行主、客体安全标记。

需要顺便说明的是,在安全信息系统中,各组成部分的安全机制一般也只能在各自的控制范围内发挥作用,这也就是所谓的“安全木桶原理”成立的基础。

**【标准条款】**

GB/T 24856—2009

**7.3.2 安全区域边界设计技术要求**

第三级安全区域边界从以下方面进行安全设计:

a) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制,实施相应的访问控制策略,对进出安全区域边界的数据信息进行控制,阻止非授权访问。

b) 区域边界包过滤

应根据区域边界安全控制策略,通过检查数据包的源地址、目的地址、传输层协议、请求的服务等,确定是否允许该数据包进出该区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制,由安全管理中心集中管理,并对确认的违规行为及时报警。

d) 区域边界完整性保护

应在区域边界设置探测器,例如外接探测软件,探测非法外联和入侵行为,并及时报告安全管理中心。

**【条款解读 27】**

一、目的和意图

描述第三级信息系统安全区域边界设计的安全技术要求。

二、解释和示例

GB/T 24856—2009 的 7.3.2(安全区域边界设计技术要求),从区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护等方面,对第三级信息系统安全区域边界设计的安全技术要求进行描述。

第三级信息系统的安全区域边界,通过安全区域边界的安全设计,对来自外部的对安全计算环境的攻击进行较高程度的安全防护,具体做法是,在第二级安全区域边界安全设

计的基础上，通过选择和配置具有符合第三级安全要求的区域边界包过滤、区域边界完整性保护和区域边界安全审计等安全机制和(或)产品，特别是增加区域边界访问控制，来进行区域边界安全防护，以对抗来自外部的攻击。

安全区域边界的访问控制与传统的操作系统和数据库管理系统的访问控制，在安全策略和主、客体标记方面应该没有多大区别，所不同的是主、客体对象的确定和访问操作的内容上。总体上讲，区域边界访问控制的主、客体粒度可能比较粗，不会像操作系统和数据库管理系统那样达到文件和库表(含记录或字段)的粒度；区域边界访问控制的主体对客体的访问操作也不会像操作系统和数据库管理系统那样达到可读、可写等程度。另外，用于安全区域边界的访问控制机制因当前还没有现成的安全产品可以实现，需要安全系统开发者在安全系统集成过程中设计和实现。

**【标准条款】**

GB/T 24856—2009

**7.3.3 安全通信网络设计技术要求**

第三级安全通信网络从以下方面进行安全设计：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。

b) 通信网络数据传输完整性保护

应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 通信网络可信接入保护

可采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

**【条款解读 28】**

一、目的和意图

描述第三级信息系统安全通信网络的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 7.3.3(安全通信网络设计技术要求)，从通信网络安全审计、通信网络数据传输完整性保护、通信网络数据传输保密性保护、通信网络可信接入等方面，对第三级信息系统安全通信网络的安全设计技术要求进行描述。

第三级信息系统的安全通信网络，通过安全通信网络的安全设计，对通信网络的安全运行和通信网络所传输的数据进行较高程度的安全保护。具体做法是，在第二级安全通信网络安全设计的基础上，通过选择和配置具有符合第三级安全要求的通信网络安全审计、通信网络数据传输完整性、保密性保护以及通信网络可信接入的安全机制和(或)产品，实现通信网络的安全保护。

在第三级信息系统的安全通信网络设计中，除了安全审计机制外，安全通信网络的数

据传输完整性保护、数据传输保密性保护和通信网络可信连接保护，目前大都采用以密码为基础的安全机制来实现。这里需要强调的是，第三级信息系统安全通信网络应采用统一的、较完整的密码体系，来实现这些安全机制。

**【标准条款】**

GB/T 24856—2009

> **7.3.4 安全管理中心设计技术要求**
>
> 7.3.4.1 系统管理
>
> 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和(或)异地灾难备份与恢复等。
>
> 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。
>
> 7.3.4.2 安全管理
>
> 应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略。
>
> 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。
>
> 7.3.4.3 审计管理
>
> 应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。
>
> 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

**【条款解读29】**

一、目的和意图

描述第三级信息系统安全管理中心的设计技术要求。

二、解释和示例

GB/T 24856—2009 的 7.3.4(安全管理中心设计技术要求)，从系统管理、安全管理、审计管理等方面，对第三级信息系统安全管理中心设计技术要求进行描述。

第三级信息系统的安全管理中心的设计，是在第二级信息系统安全管理中心设计的基础上，通过增强对安全审计的管理和增加安全管理的相关内容，实现信息系统各安全机制的统一管理。第三级信息系统各安全机制的统一管理主要包括：对系统中由安全策略控制的主体、客体进行统一标记，对主体进行统一授权管理，并为全系统配置统一的安全策略；对分布在系统中的各种需要集中控制和管理的安全机制进行管理和控制；实现系统管理员、安全员和审计员的三权分离，并形成相互制约关系；为安全员和审计员各自提供专用的操作界面，按照第三级安全的要求进行身份鉴别，并对其操作行为进行安全审计。

安全管理中心的设计，可以选择市场上已有的相应产品进行集成，也可以在系统集成过程中进行设计。市场上的相应产品一般是指对分布式安全机制具有集中管理和控制功

能的产品。这类产品目前常见的有：具有集中管控功能的安全审计产品，具有分布式管理功能的安全监控产品，以及进行集中身份鉴别的单点登录等。对于需要进行统一的主、客体标记这样一些安全功能的，一般需要在安全系统集成过程中进行设计。这里需要强调的是，在选择已有产品时应注意其接口的标准化和一致性，以免带来不必要的麻烦。

## 1.6 第四级信息系统安全保护环境设计

**【标准条款】**

GB/T 24856—2009

> **8 第四级系统安全保护环境设计**

**【条款解读 30】**

一、目的和意图

描述第四级信息系统安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 8 章(第四级系统安全保护环境设计)，从设计目标、设计策略和设计技术要求等方面，对第四级信息系统的安全保护环境的安全设计要求进行描述。

有关第四级系统安全保护环境安全设计要求的进一步解释，参见条款解读 31～条款解读 33。

### 1.6.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **8.1 设计目标**
>
> 第四级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第四级系统的安全保护要求，建立一个明确定义的形式化安全策略模型，将自主和强制访问控制扩展到所有主体与客体，相应增强其他安全功能强度；将系统安全保护环境结构化为关键保护元素和非关键保护元素，以使系统具有抗渗透的能力。

**【条款解读 31】**

一、目的和意图

描述第四级信息系统安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 8.1(设计目标)，对第四级信息系统安全保护环境的安全设计

目标进行描述。强调第四级信息系统安全保护环境的安全设计是对 GB 17859—1999 结构化保护级安全保护要求的具体实现，是在第三级信息系统安全保护环境的安全环境安全设计的基础上，把标记和强制访问控制的范围扩展到系统的所有主、客体，并从结构化设计的角度增强信息系统安全保护的强度。安全设计目标是达到整个信息系统的安全保护能力以能够抵御各种内、外部攻击。

第四级信息系统安全保护环境的安全设计目标，应根据信息安全等级保护的有关政策法规（如公通字[2004]66 号文件和公通字[2007]43 号文件等）对第四级信息系统安全要求的描述，按照风险分析方法所确定的目标信息系统的安全需求，以及信息安全等级保护相关标准对适用于第四级信息系统的安全要素和安全产品的具体要求，综合分析进行确定。

## 1.6.2 安全设计策略

**【标准条款】**

GB/T 24856—2009

> **8.2 设计策略**
>
> 第四级系统安全保护环境的设计策略是：在第三级系统安全保护环境设计的基础上，遵循 GB 17859—1999的 4.4 中相关要求，通过安全管理中心明确定义和维护形式化的安全策略模型。依据该模型，采用对系统内的所有主、客体进行标记的手段，实现所有主体与客体的强制访问控制。同时，相应增强身份鉴别、审计、安全管理等功能，定义安全部件之间接口的途径，实现系统安全保护环境关键保护部件和非关键保护部件的区分，并进行测试和审核，保障安全功能的有效性。
>
> 第四级系统安全保护环境的设计通过第四级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

**【条款解读 32】**

一、目的和意图

描述第四级信息系统安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 8.2（设计策略），强调第四级信息系统安全保护环境的安全设计应遵循 GB 17859—1999 的 4.4 的相关要求，在第三级信息系统安全保护环境安全设计的基础上，通过安全管理中心，明确定义和维护形式化的安全策略模型，对系统内的所有主、客体进行标记和强制访问控制，并对数据存储和传输保护等其他安全功能采取更加有效的措施；具体做法是通过对安全计算环境、安全区域边界、安全通信网络的安全设计，以及安全管理中心的设计，实现第四级信息系统安全保护环境的安全设计目标。

在第四级信息系统安全保护环境的安全设计中，安全策略应是对实现第四级信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

## 1.6.3 安全设计技术要求

**【标准条款】**

GB/T 24856—2009

| 8.3 设计技术要求 |
| --- |

**【条款解读 33】**

一、目的和意图

描述第四级信息系统安全保护环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 8.3(设计技术要求),从安全计算环境安全设计、安全区域边界安全设计、安全通信网络安全设计、安全管理中心设计和系统安全保护环境结构化设计等方面,对第四级信息系统安全保护环境的安全设计技术要求进行描述。

计算环境和通信网络是信息系统不可缺少的组成部分。第四级安全计算环境,是按照所确定的第四级信息系统安全保护环境的安全设计目标和安全设计策略对安全计算环境的安全要求,在计算环境所实现的计算功能的基础上,附加实现相应安全保护功能的对计算环境进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全计算环境;第四级安全通信网络,是按照所确定的第四级信息系统安全保护环境的安全设计目标和安全设计策略对通信网络的安全要求,在通信网络所实现的通信功能的基础上,附加实现相应安全保护功能的对通信网络功能进行安全保护的安全技术和机制构成的具有相应安全保护能力的安全通信网络。

安全区域边界是专为在安全计算环境的边界进行安全保护而设置的。第四级安全区域边界是按照确定的第四级信息系统安全保护环境的安全设计目标和安全设计策略对区域边界的安全要求,采用具有相应安全保护能力的安全技术和安全产品构成的区域边界。

安全管理中心是专为信息系统安全保护环境进行集中管理设置的。第四级信息系统安全保护环境的安全管理中心统一管理和控制系统的安全策略和所有分布式安全机制,包括进行所有主客体的统一标记、主体授权管理和强制访问控制,以及分散在系统各组成部分的所有安全机制的统一管理和配置。

安全计算环境、安全区域边界和安全通信网络三者中的安全机制,在安全管理中心的管理之下,实施统一的安全策略,协同运行,共同实现第四级信息系统的安全保护目标。

第四级信息系统的安全计算环境,应对信息系统进行更高程度的安全保护,在第三级安全保护环境安全设计的基础上,通过安全保护环境的结构化设计,使系统的抗攻击能力提高到一个更高的水平;在安全机制方面,要求将标记和强制访问控制的范围扩展到系统所有的主、客体;在用户身份鉴别和用户数据的完整性保护和保密性保护等方面,应有更大的增强。比如,采用完整的高强度的密码体系,实现用户身份鉴别、签名、验证、抗抵赖,用户数据的保密性、完整性保护,以及程序可信执行保护和通信网络可信接入等,并通过完整的安全管理中心实现对整个信息系统安全保护环境安全策略的统一管理。

有关第四级信息系统安全保护环境的安全设计技术要求的进一步解释，参见条款解读34～条款解读38。

**【标准条款】**

GB/T 24856—2009

**8.3.1 安全计算环境设计技术要求**

第四级安全计算环境从以下方面进行安全设计：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，将强制访问控制扩展到所有主体与客体；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，终止违例进程等；确保审计记录不被破坏或非授权访问以及防止审计记录丢失等。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。

g) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源在重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h) 程序可信执行保护

应构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等的攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

## 【条款解读 34】

一、目的和意图

描述第四级信息系统安全计算环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 8.3.1(安全计算环境设计技术要求),从用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、程序可信执行保护等方面,对第四级信息系统安全计算环境设计的技术要求进行描述。

第四级信息系统的安全计算环境,要求对计算环境进行较高程度的安全保护,选择具有第四级安全的操作系统和数据库管理系统实现对安全计算环境的安全保护。第四级安全的操作系统应符合 GB/T 20272—2006《信息安全技术 操作系统安全技术要求》的 4.4 关于第四级安全操作系统的基本要求;第四级安全的数据库管理系统应符合 GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》的 5.4 关于第四级安全数据库管理系统的基本要求。在第三级安全设计的基础上,在操作系统和数据库管理系统中,通过将实施标记和强制访问控制的范围扩展到系统中的所有主、客体,使系统具有整体的抗攻击能力,同时要求在用户身份鉴别和用户数据的完整性保护和保密性保护等方面也有相应的提升。比如,采用完整的高强度的密码体系,实现用户身份鉴别、签名、用户数据的保密性、完整性保护,以及程序可信执行保护等。

第四级信息系统安全计算环境的安全设计与第三级信息系统安全计算环境的安全设计的一个明显的区别是要求将"自主和强制访问控制扩展到所有主体与客体"。而在第三级信息系统安全计算环境的安全设计中,自主和强制访问控制只是对所确定的主体与客体实施。如何正确理解这一要求,成为第四级信息系统安全保护环境安全设计的关键。

在 GB 17859—1999 中第四级的相关要求是:"可信计算基对外部主体能够直接或间接访问的所有资源(例如:主体、存储客体和输入/输出资源)实施强制访问控制,为这些主体及客体指定敏感标记。这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。"第三级的相关要求是:"可信计算基对所有主体及其所控制的客体(例如:进程、文件、段、设备)实施强制访问控制,为这些主体及客体指定敏感标记。"第四级的核心是强调对系统中的"所有资源"实施强制访问控制。如果把这种强制访问控制要求看作是对系统中"所有"资源的高的安全保护要求的表征,那么在第四级信息系统的安全计算环境的安全设计中,其他相关的安全要素,如用户身份鉴别、用户数据的完整性、保密性保护等安全技术和机制,都应对其所控制的"所有资源"提供与强制访问控制具有相当安全强度的安全保护。这种对系统中"所有资源"的高安全保护要求,同样可以扩展到第四级信息系统的安全区域边界和安全通信网络。

## 【标准条款】

GB/T 24856—2009

> **8.3.2 安全区域边界设计技术要求**
>
> 第四级安全区域边界从以下方面进行安全设计：
>
> a) 区域边界访问控制
>
> 应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。
>
> b) 区域边界包过滤
>
> 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界。
>
> c) 区域边界安全审计
>
> 应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警并作出相应处置。
>
> d) 区域边界完整性保护
>
> 应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

## 【条款解读 35】

一、目的和意图

描述第四级信息系统安全区域边界设计的安全技术要求。

二、解释和示例

GB/T 24856—2009 的 8.3.2(安全区域边界设计技术要求)，从区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护等方面，对第四级信息系统安全区域边界设计的安全技术要求进行描述。

第四级信息系统的安全区域边界，通过安全区域边界的安全设计，对来自外部的对安全计算环境的攻击进行更高程度的安全防护。具体做法是，在第三级安全区域边界安全设计的基础上，通过选择和配置具有符合第四级安全要求的区域边界访问控制、区域边界包过滤、区域边界完整性保护和区域边界安全审计等安全机制和产品，来进行区域边界安全防护，以对抗来自外部的攻击。

按照第四级信息系统安全计算环境安全设计中对系统中的“所有资源”实施强制访问控制的要求，在第四级信息系统安全区域边界的安全设计中，其强制访问控制和其他安全要素，都应对其所控制的“所有资源”提供与强制访问控制具有相当安全强度的安全保护。

## 【标准条款】

GB/T 24856—2009

> **8.3.3 安全通信网络设计技术要求**
>
> 第四级安全通信网络从以下方面进行安全设计：
>
> a) 通信网络安全审计
>
> 应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警，且作出相应处置。

b) 通信网络数据传输完整性保护

应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 通信网络可信接入保护

应采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

## 【条款解读 36】

一、目的和意图

描述第四级信息系统安全通信网络安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 8.3.3(安全通信网络设计技术要求)，从通信网络安全审计、通信网络数据传输完整性保护、通信网络数据传输保密性保护、通信网络可信接入等方面，对第四级信息系统安全通信网络的安全设计技术要求进行描述。

第四级信息系统的安全通信网络，通过安全通信网络的安全设计，对通信网络的安全运行和通信网络所传输的数据进行更高程度的安全保护，具体做法是，在第三级安全通信网络安全设计的基础上，通过选择和配置具有符合第四级安全要求的通信网络安全审计、通信网络数据传输完整性、保密性保护以及通信网络可信接入的安全机制和(或)产品，实现通信网络的安全保护。

按照第四级信息系统安全计算环境安全设计中对系统中的“所有资源”实施强制访问控制的要求，在第四级信息系统安全通信网络的安全设计中的安全要素，都应对其所控制的“所有资源”提供与强制访问控制具有相当安全强度的安全保护。

## 【标准条款】

GB/T 24856—2009

**8.3.4 安全管理中心设计技术要求**

8.3.4.1 系统管理

应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和异地灾难备份与恢复等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

8.3.4.2 安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略，并确保标记、授权和安全策略的数据完整性。

应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

> 8.3.4.3 审计管理
>
> 应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。
>
> 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

**【条款解读37】**

一、目的和意图

描述第四级信息系统安全管理中心设计的技术要求。

二、解释和示例

GB/T 24856—2009的8.3.4(安全管理中心技术设计要求)，从系统管理、安全管理、审计管理等方面，对第四级信息系统安全管理中心设计技术要求进行描述。

第四级信息系统的安全管理中心的设计，是在第三级信息系统安全管理中心设计的基础上，通过增强对安全审计和安全管理的相关内容，实现信息系统各安全机制的统一管理。第四级信息系统各安全机制的统一管理主要包括：对系统中的所有主体、客体进行统一标记，对主体进行统一授权管理，并为全系统配置统一的安全策略；对分布在系统中的各种需要集中控制和管理的安全机制进行管理和控制；实现系统管理员、安全员和审计员的三权分离，并形成相互制约关系；为安全员和审计员各自提供专用的操作界面，并对安全员和审计员按照第四级安全的要求进行严格的身份鉴别，对其操作行为进行审计。

**【标准条款】**

GB/T 24856—2009

> **8.3.5 系统安全保护环境结构化设计技术要求**
>
> 8.3.5.1 安全保护部件结构化设计技术要求
>
> 第四级系统安全保护环境各安全保护部件的设计应基于形式化的安全策略模型。安全保护部件应划分为关键安全保护部件和非关键安全保护部件，防止违背安全策略致使敏感信息从关键安全保护部件流向非关键安全保护部件。关键安全保护部件应划分功能层次，明确定义功能层次间的调用接口，确保接口之间的信息安全交换。
>
> 8.3.5.2 安全保护部件互联结构化设计技术要求
>
> 第四级系统各安全保护部件之间互联的接口功能及其调用关系应明确定义；各安全保护部件之间互联时，需要通过可信验证机制相互验证对方的可信性，确保安全保护部件间的可信连接。
>
> 8.3.5.3 重要参数结构化设计技术要求
>
> 应对第四级系统安全保护环境设计实现的与安全策略相关的重要参数的数据结构给出明确定义，包括参数的类型、使用描述以及功能说明等，并用可信验证机制确保数据不被篡改。

**【条款解读38】**

一、目的和意图

描述第四级信息系统安全保护环境结构化设计技术要求。

二、解释和示例

GB/T 24856—2009 的 8.3.5(系统安全保护环境结构化设计技术要求),从安全保护部件结构化设计、安全保护部件互联结构化设计、重要参数结构化设计等方面,对安全保护环境结构化设计的技术要求进行描述。

安全机制是操作系统安全的基础,也是信息系统安全的核心。然而,即使信息系统中存在非常完善的安全机制,但是如果信息系统的各组成模块间的接口关系不清晰,逻辑和调用关系混乱,那么系统中就及可能存在隐蔽通道,致使攻击者可以绕过系统的安全机制访问客体资源,使得系统中的重要信息缺乏基础安全保障。相反,如果信息系统在设计时明确定义了各组成模块的功能,并且依据一个严谨的安全体系结构确定了模块间的接口关系,同时利用相应的方法验证了每一模块的工程实现都是正确的,没有引入新的接口,这样就可以保证系统中的所有信息流都是预先设计好的,避免出现隐蔽通道,也就避免了系统安全机制被旁路的风险。因此,对于高等级信息系统开发而言,最大的难点不在于安全功能的实现,而在于安全保证机制的实现,即确保系统的 TCB 始终有效、不被旁路。基于上述原因,GB 17859—1999 对四级以上信息系统提出了结构化保证的要求。因此,高等级信息系统结构化保证技术是本课题研究需要解决的主要内容之一。

本课题拟从安全程序结构化、重要数据结构化、连接交互结构化三个方向入手,实现对重要信息系统的结构化保证。其中安全程序结构化主要针对安全部件,实现系统层次清晰化、系统功能模块化、函数调用单向化;重要数据结构化主要实现系统数据的结构化保护,包括策略模型的形式化、系统关键数据结构的局部化、程序对关键数据结构访问的范围控制,以及数据在不同层次之间的传输;连接交互结构化用于保证安全部件 TCB 的无缝连接,完成从安全部件 TCB 出发,通过基于隔离保护机制的 TCB 扩展,将 TCB 扩展到整个系统的过程。

对结构化的上述三个方向而言,Linux 操作系统的安全程序结构化改造是本课题在结构化保证技术研究方面的重点。对 Linux 进行结构化改造拟通过对操作系统进行层次划分和实现层次间的单向调用关系来完成,如图 1-2 所示。首先,分析 Linux 操作系统的

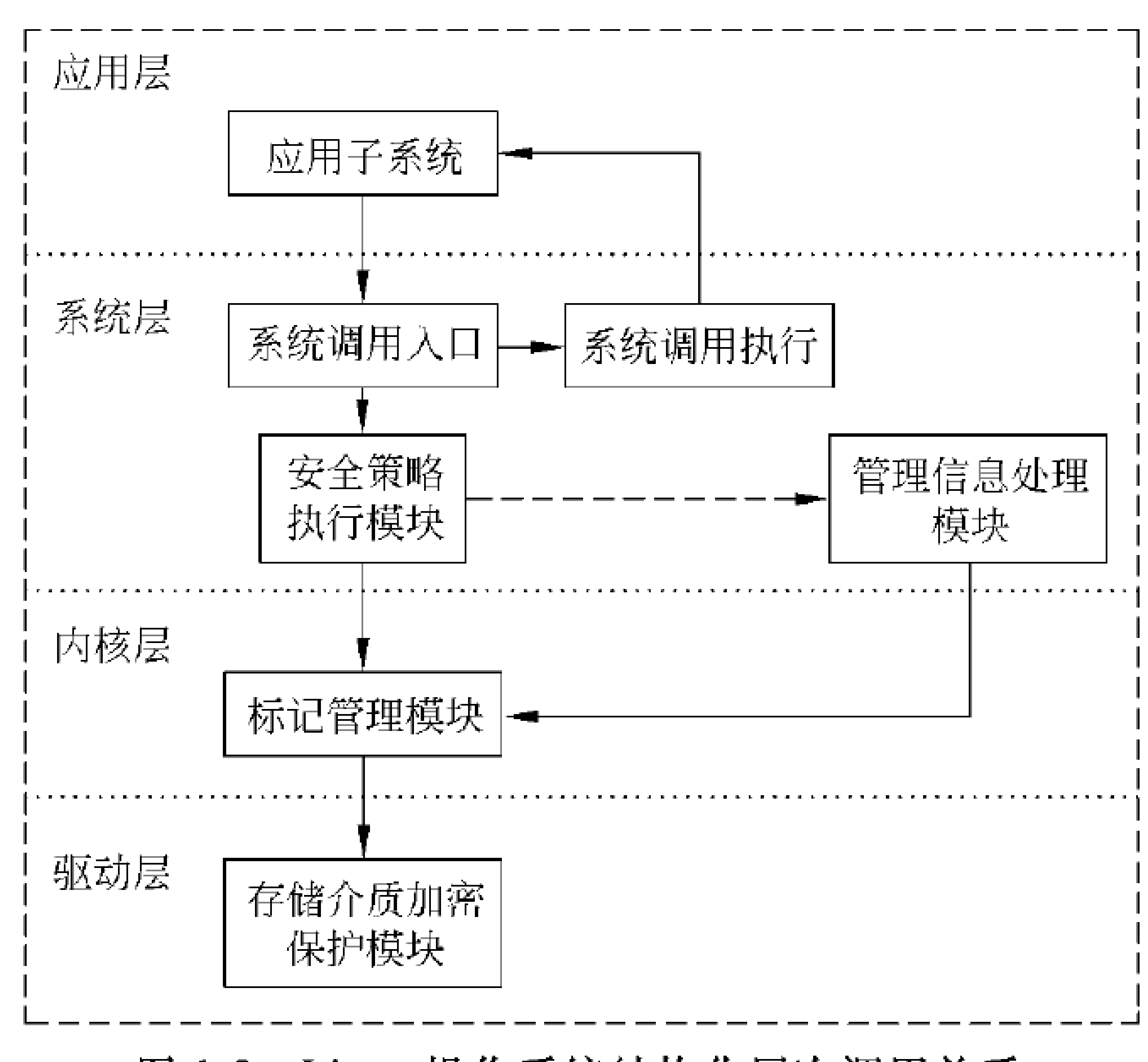
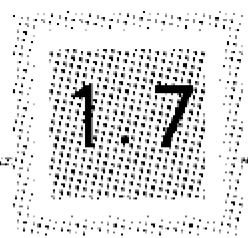



图 1-2　Linux 操作系统结构化层次调用关系

组成模块，明确各模块的功能和其间的接口关系，分离系统关键安全部件与其他部件，完成操作系统内核的层次化改造，将系统划分为应用层、系统层、内核层和驱动层。其次，通过层次间调用关系检查机制保障层次间的单向调用关系，保证系统在正常运行状态时，应用层、系统层、内核层和驱动层之间的相对隔离。这样，就可以保证操作系统建立在一个明确的层次化的安全体系结构之上，各层次之间的信息流都经过安全检查，确保系统中不会有非预期的信息流存在。



## 1.7 第五级信息系统安全保护环境设计

**【标准条款】**

GB/T 24856—2009

| |
|---|
| **9 第五级系统安全保护环境设计** |

**【条款解读 39】**

一、目的和意图

描述第五级信息系统安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 9 章(第五级系统安全保护环境设计)，从设计目标、设计策略和设计技术要求等方面，对第五级信息系统的安全保护环境设计的要求进行简要描述。

有关第五级系统安全保护环境设计要求的进一步解释，参见条款解读 40～条款解读 42。

### 1.7.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **9.1 设计目标**
>
> 第五级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第五级系统的安全保护要求，在第四级系统安全保护环境的基础上，实现访问监控器，仲裁主体对客体的访问，并支持安全管理职能。审计机制可根据审计记录及时分析发现安全事件并进行报警，提供系统恢复机制，以使系统具有更强的抗渗透能力。

**【条款解读 40】**

一、目的和意图

描述第五级信息系统安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 9.1(设计目标),对第五级信息系统安全保护环境的安全设计目标进行描述。强调第五级信息系统安全保护环境的安全设计是对 GB 17859—1999 访问验证保护级安全保护要求的具体实现,是在第四级信息系统安全保护环境设计的基础上,在安全专控部门的指导下进行安全保护环境的设计。安全设计目标是达到安全专控部门所要求的安全保护能力的水平。

第五级信息系统安全保护环境的安全设计目标,应根据信息安全等级保护有关政策法规(如公通字[2004]66 号文件和公通字[2007]43 号文件等)对第五级信息系统安全要求的描述,按照风险分析的方法所确定的目标信息系统的安全需求,以及信息安全等级保护相关标准对适用于第五级信息系统的安全要素和安全产品的具体要求,综合分析进行确定。

## 1.7.2 安全设计策略

**【标准条款】**

GB/T 24856—2009

> **9.2 设计策略**
>
> 第五级系统安全保护环境的设计策略是:遵循 GB 17859—1999 的 4.5 中"访问监控器本身是抗篡改的;必须足够小,能够分析和测试"。在设计和实现访问监控器时,应尽力降低其复杂性;提供系统恢复机制;使系统具有更强的抗渗透能力;所设计的访问监控器能进行必要的分析与测试,具有抗篡改能力。
>
> 第五级系统安全保护环境的设计通过第五级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

**【条款解读 41】**

一、目的和意图

描述第五级信息系统安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 9.2(设计策略),强调第五级信息系统安全保护环境的安全设计应遵循 GB 17859—1999 的 4.5 的相关要求,在第四级信息系统安全保护环境安全设计的基础上,要求访问监控器本身是抗篡改的、必须足够小、能够分析和测试,并在设计和实现时尽量降低复杂性,使系统具有很高的抗渗透能力,并使安全系统具有自身恢复的能力;具体通过对安全计算环境、安全区域边界、安全通信网络的安全设计,以及安全管理中心的设计,实现第五级信息系统安全保护环境的安全设计目标。

在第五级信息系统安全保护环境的安全设计中,安全策略应是对实现第五级信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

### 1.7.3 安全设计技术要求

**【标准条款】**

GB/T 24856—2009

> **9.3 设计技术要求**

第五级系统安全保护环境设计技术要求另行制定。

**【条款解读 42】**

一、目的和意图

指出第五级信息系统安全保护环境的安全设计技术要求需要另行制定。

二、解释和示例

GB/T 24856—2009 的 9.3(设计技术要求),指出第五级信息系统安全保护环境的安全设计技术要求需要根据有关规定,由有关职能部门另行制定。

## 1.8 信息系统互联安全保护环境设计

**【标准条款】**

GB/T 24856—2009

> **10 定级系统互联设计**

**【条款解读 43】**

一、目的和意图

描述不同安全等级信息系统之间互联安全保护环境的安全设计要求。

二、解释和示例

GB/T 24856—2009 的第 10 章(定级系统互联设计),从设计目标、设计策略和设计技术要求等方面,对不同安全等级信息系统之间互联的安全保护环境的安全设计要求进行描述。

有关信息系统互联安全保护环境的安全设计要求的进一步解释,参见条款解读 44~条款解读 46。

### 1.8.1 安全设计目标

**【标准条款】**

GB/T 24856—2009

> **10.1 设计目标**
>
> 定级系统互联的设计目标是:对相同或不同等级的定级系统之间的互联、互通、互操作进行安

全保护，确保用户身份的真实性、操作的安全性以及抗抵赖性，并按安全策略对信息流向进行严格控制，确保进出安全计算环境、安全区域边界以及安全通信网络的数据安全。

【条款解读 44】

一、目的和意图

描述信息系统互联安全保护环境的安全设计目标。

二、解释和示例

GB/T 24856—2009 的 10.1(设计目标)，对相同或不同安全等级信息系统之间互联保护环境的安全设计目标进行描述。指出不同或相同安全保护等级系统之间互联的安全设计目标是确保进出安全计算环境、安全区域边界以及安全通信网络的数据安全保护能力，以及各安全计算环境对外部攻击的抵御能力达到其应具有的安全水平。

## 1.8.2 安全设计策略

【标准条款】

GB/T 24856—2009

**10.2 设计策略**

定级系统互联的设计策略是：遵循 GB 17859—1999 对各级系统的安全保护要求，在各定级系统的计算环境安全、区域边界安全和通信网络安全的基础上，通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护。

【条款解读 45】

一、目的和意图

描述信息系统互联安全保护环境的安全设计策略。

二、解释和示例

GB/T 24856—2009 的 10.2(设计策略)，对相同或不同安全等级信息系统之间互联安全保护环境的安全设计策略进行描述。指出通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护，达到各安全等级的系统之间实现安全互联的目标。

在信息系统互联安全保护环境的具体设计中，安全策略应是对实现信息系统安全保护环境安全功能的安全技术、机制、原理和方法的完整描述。

## 1.8.3 安全设计技术要求

【标准条款】

GB/T 24856—2009

**10.3 设计技术要求**

**【条款解读 46】**

一、目的和意图

描述信息系统互联安全保护环境的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 10.3(设计技术要求),从安全互联部件设计技术要求、跨定级系统安全管理中心设计技术要求等方面,对信息系统互联安全保护环境的安全设计技术要求进行描述。

有关信息系统互联安全保护环境的安全设计技术要求的进一步解释,参见条款解读 47和条款解读 48。

**【标准条款】**

GB/T 24856—2009

> **10.3.1 安全互联部件设计技术要求**
>
> 应通过通信网络交换网关与各定级系统安全保护环境的安全通信网络部件相连接,并按互联互通的安全策略进行信息交换,实现安全互联部件。安全策略由跨定级系统安全管理中心实施。

**【条款解读 47】**

一、目的和意图

描述信息系统互联安全保护环境安全互联部件的安全设计技术要求。

二、解释和示例

GB/T 24856—2009 的 10.3.1(安全互联部件设计技术要求),对信息系统互联安全保护环境的安全设计技术要求进行描述。

信息系统互联安全保护环境的安全互联部件的设计,主要是对“通信网络交换网关”的设计,该网关通过实施由跨定级系统安全管理中心统一控制和管理的安全策略,实现多级安全互联的安全要求。

多级安全互联是以各级安全应用平台自身安全保护为基础,辅以相关的互联网络的安全机制,实现多级安全应用平台之间的操作和数据传输与交换的安全保护。这些安全机制主要包括:身份鉴别、访问控制、区域边界防护、数据传输安全保护、抗抵赖(行为不可否认)性、系统可用性,以及可信连接等。

**【标准条款】**

GB/T 24856—2009

> **10.3.2 跨定级系统安全管理中心设计技术要求**
>
> 应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连,主要实施跨定级系统的系统管理、安全管理和审计管理。
>
> 10.3.2.1 系统管理
>
> 应通过系统管理员对安全互联部件与相同和不同等级的定级系统中与安全互联相关的系统资源和运行进行配置和管理,包括用户身份管理、安全互联部件资源配置和管理等。

10.3.2.2　安全管理

应通过安全管理员对相同和不同等级的定级系统中与安全互联相关的主/客体进行标记管理，使其标记能准确反映主/客体在定级系统中的安全属性；对主体进行授权，配置统一的安全策略，并确保授权在相同和不同等级的定级系统中的合理性。

10.3.2.3　审计管理

应通过安全审计员对安全互联部件的安全审计机制、各定级系统的安全审计机制以及与跨定级系统互联有关的安全审计机制进行集中管理。包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。

**【条款解读 48】**

一、目的和意图

描述信息系统互联安全保护环境的跨定级系统安全管理中心设计技术要求。

二、解释和示例

GB/T 24856—2009 的 10.3.2(跨定级系统安全管理中心设计技术要求)，从系统管理、安全管理和审计管理等方面，对信息系统互联安全保护环境的跨定级系统安全管理中心设计技术要求进行描述。

多级安全互联是指通过不同安全等级的安全应用平台之间的安全连接，为不同安全平台之间的互操作提供安全支持，既要确保进行操作的用户身份的真实性和操作的合法性，又要确保数据出/入安全计算环境的合法性和数据在传输过程中的安全性。

多级安全互联是以各级安全应用平台自身安全保护为基础，辅以相关的互联网络的安全机制，实现多级安全应用平台之间的操作和数据传输与交换的安全保护。这些安全机制主要包括：身份鉴别、访问控制、区域边界防护、数据传输安全保护、抗抵赖(行为不可否认)性、系统可用性，以及可信连接等。

以下是多级互联安全方案设计的示例。

多级互联网关的拓扑结构如图 1-3 所示，各级互联网网关部署在专网区域边界，隔离专网与公网，以基于等级标记的安全互联协议来进行公网上的通信网络。

1. 拓扑结构图

2. 安全功能

(1) 互联网关功能

各级互联安全网关基于等级标记信息实施通信网络访问控制。等级标记包括等级ID，指明等级级别，发起连接的主体标识，关联的范畴信息，安全计算环境的安全状态与配置信息等。互联安全功能如下所述。

① 专网接出：解析内部连接 IP 等级标记信息，分析主体信息，与专网用户管理系统等联动确定主体访问权限，确定主体能否外连接出。

② 专网接入：解析外部连接 IP 等级标记信息，分析主体信息，与全局安全基础设施、管理中心等联动确定主体访问权限，确定主体能否外连接入，如能接入，则与访问控制代理联动分配代理主体，确定权限，已定义的访问控制规则由代理主体访问专网。

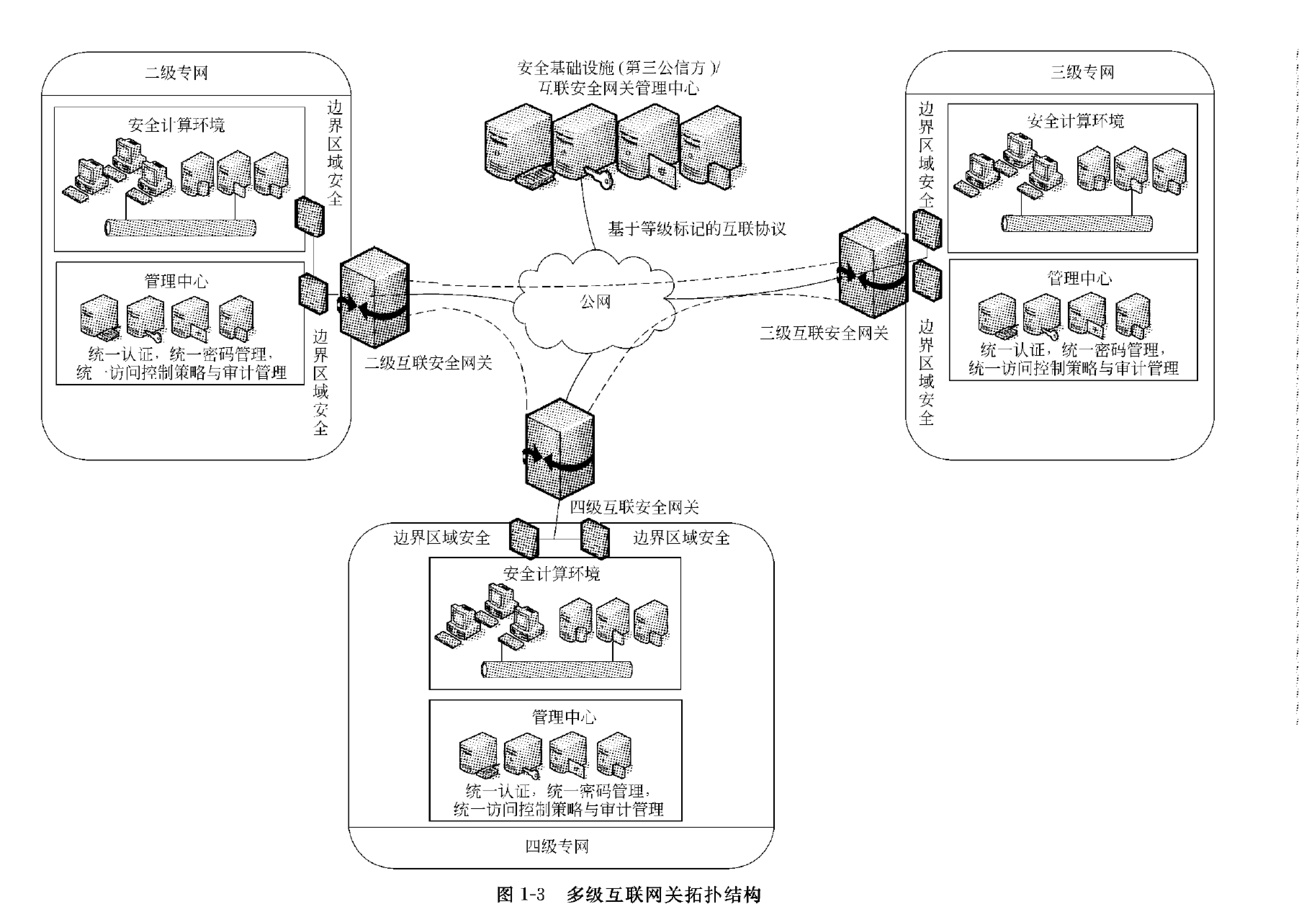



图 1-3　多级互联网关拓扑结构

③ 对接入接出事件实施审计。

④ 管理功能，包括：

- 接入/接出通信网络访问控制策略管理；
- 基于等级标记的安全互联协议配置管理；
- 证书等密码管理；
- 安全管理员的认证管理。

多级互联安全网关的自身安全由基于可信安全计算机的硬件平台结合相应级别的安全操作系统来保证，具体指标是保持与其管理的专网级别一致。

(2) 互联网关协议

互联网关协议需要保证：

① 数据完整性——验证数据在传输、处理时是否被修改；

② 实体标识和认证——证明安全互联网关身份，证实消息的原发者；

③ 行为不可否认性——提供通信双方不可否认的参与证明；

④ 数据保密性——用密码加密方式保证数据在传输和处理时的秘密性；

⑤ 系统可用性——保证数据的传输和计算处理不拒绝授权用户的访问；

⑥ 数据可用性——保证不同等级信息的安全流动和操作。

互联网关协议以我国自主研制的 TNC 协议为基础进行设计。

(3) 专网

专网的安全计算环境提供等级标记的实现与管理，为了实现多级互联，专网需要实现如下功能：

① 对接入/接出的主体能够标识，能够对主体进行认证与授权；

② 能够定义全网的安全策略，确定内部主体、代理外部主体的访问控制规则并实施资源控制；

③ 对主体行为实施审计；

④ 等级标记的实现、配置和管理；

⑤ 内部子网的多级互联管理与策略配置。

(4) 安全基础设施(第三方公信方)/安全管理中心

安全基础设施提供如下服务：

① PKI/CA 的证书服务；

② 认证中心；

③ PMI；

④ 密码服务。

安全管理中心提供如下服务：

① 安全互联网关的策略配置；

② 等级标记的全局管理；

③ 审计管理。

3. 系统组成

(1) 二级安全互联网关的组成

二级安全互联网关由以下部分组成：

① 多级安全互联通信网络访问控制软件；

② 实现了自主访问控制、客体重用、身份鉴别等安全功能的二级操作系统；

③ 安全强度达到二级要求的可信计算硬件平台。

(2) 三级安全互联网关的组成

三级安全互联网关由以下部分组成：

① 多级安全互联通信网络访问控制软件；

② 实现了自主访问控制、强制访问控制、客体重用、身份鉴别等安全功能的三级安全操作系统；

③ 安全强度达到三级要求的可信计算硬件平台。

(3) 四级安全互联网关的组成

四级安全互联网关由以下部分组成：

① 多级安全互联通信网络访问控制软件；

② 四级安全操作系统；

③ 安全强度达到四级要求的可信计算硬件平台。

在上述多级互联安全方案设计中涉及以下主要技术：

① 多级可信互联模型和多级安全互联体系结构；

② 基于标记的跨级跨区域可信互联技术；

③ 区域内部跨级数据安全交换技术；

④ 跨级跨系统认证、授权与访问控制技术；

⑤ 跨级访问策略冲突检测消解技术；

⑥ 支持多级之间任意互联的多级安全互联技术。

## 1.9 访问控制机制设计

**【标准条款】**

GB/T 24856—2009

| |
|---|
| **附录 A(资料性附录)访问控制机制设计** |

**【条款解读 49】**

一、目的和意图

以资料性附录的形式，给出自主访问控制机制设计和强制访问控制设计的基本方法。

二、解释和示例

GB/T 24856—2009 的附录 A(访问控制机制设计)，包括自主访问控制设计和强制访问控制设计，共两节，下面分别对 A.1 和 A.2 进行解释。

有关系统安全互联设计技术要求的进一步解释，参见条款解读 50 和条款解读 51。

## 1.9.1 自主访问控制设计

**【标准条款】**

GB/T 24856—2009

**A.1 自主访问控制机制设计**

系统在初始配置过程中，安全管理中心首先需要对系统中的主体及客体进行登记命名，然后根据自主访问控制安全策略，按照主体对其创建客体的授权命令，为相关主体授权，规定主体允许访问的客体和操作，并形成访问控制列表。自主访问控制机制结构如图 A-1 所示。

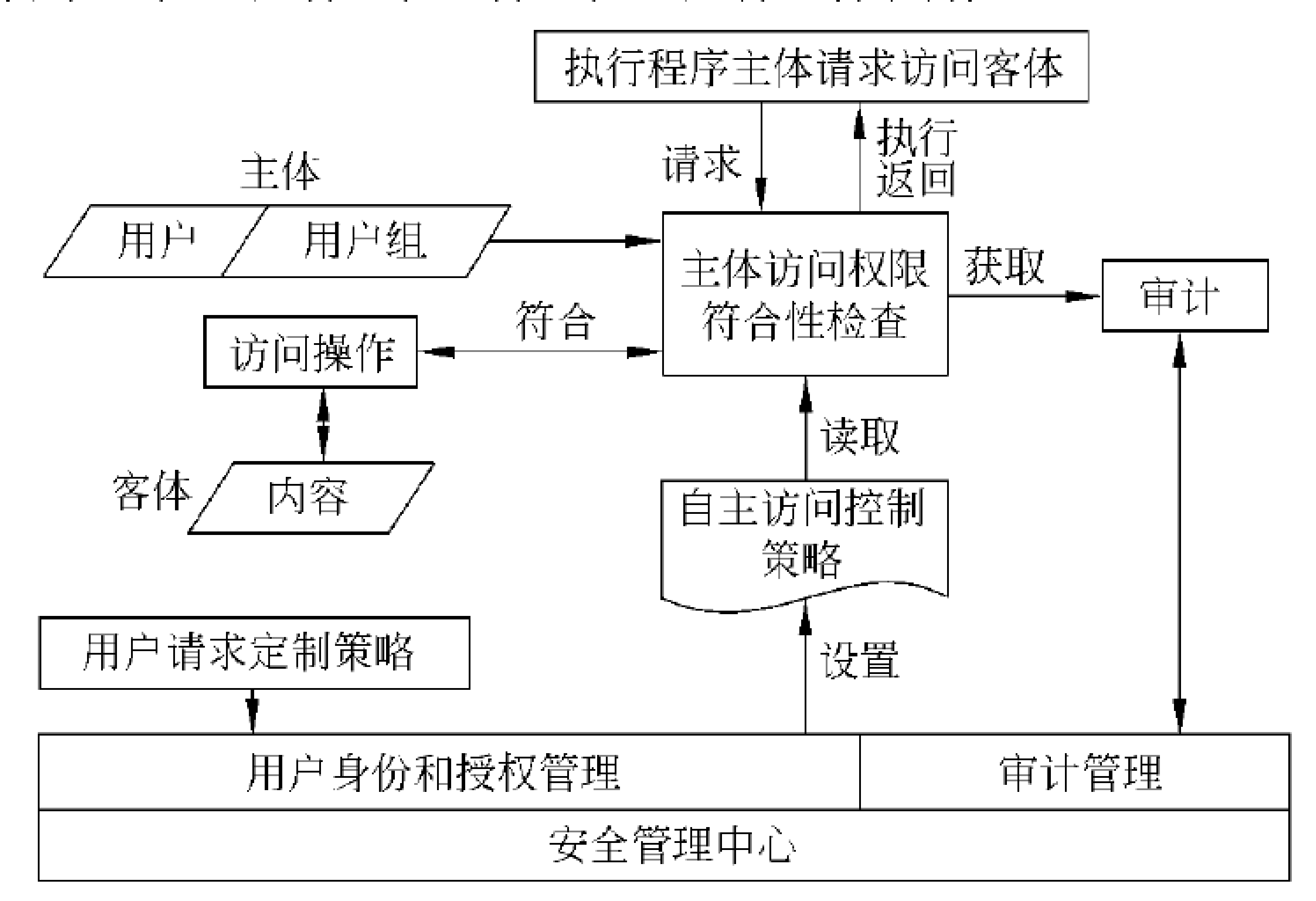



图 A-1 自主访问控制机制结构

用户登录系统时，首先进行身份鉴别，经确认为合法的注册用户可登录系统，并执行相应的程序。当执行程序主体发出访问系统中客体资源的请求后，自主访问控制安全机制将截获该请求，然后查询对应的访问控制列表。如果该请求符合自主访问控制列表规定的权限，则允许其执行；否则将拒绝执行，并将此行为记录在审计记录中。

**【条款解读 50】**

一、目的和意图

描述自主访问控制设计的基本方法和结构。

二、解释和示例

GB/T 24856—2009 的附录 A.1(自主访问控制机制设计)，对自主访问控制机制的结构和处理流程进行了描述。

操作系统的访问控制是操作系统安全控制保护中的重要一环。它是在身份识别的基础上，根据身份对提出的资源访问请求加以控制。用户只能根据自己的权限大小来访问系统资源，而不能越权访问。

文件或数据管理系统采用的访问控制的一个通用工具是访问矩阵，见表 1-1。矩阵的一维由用户标识组成，另一维列出了可被访问的对象。矩阵中的每一项指明了该用户对该对象的访问权限。

对用户身份、应用数据的权限、系统资源的标记等进行统一安全管理，实现系统的整体安全控制。

**表 1-1 访问矩阵**

| | File1 | File2 | File3 | File4 |
|---|---|---|---|---|
| User_a | R,W,X | | R,W,X | |
| User_b | R | R,W,X | W | R |
| User_c | R,W | R | | R,W,X |

## 1.9.2 强制访问控制设计

### 【标准条款】

GB/T 24856—2009

**A.2 强制访问控制机制设计**

系统在初始配置过程中，安全管理中心需要对系统中的确定主体及其所控制的客体实施身份管理、标记管理、授权管理和策略管理。身份管理确定系统中所有合法用户的身份、工作密钥、证书等与安全相关的内容。标记管理根据业务系统的需要，结合客体资源的重要程度，确定系统中所有客体资源的安全级别及范畴，生成全局客体安全标记列表；同时根据用户在业务系统中的权限和角色确定主体的安全级别及范畴，生成全局主体安全标记列表。授权管理根据业务系统需求和安全状况，授予用户访问客体资源的权限，生成强制访问控制策略和级别调整策略列表。策略管理则根据业务系统的需求，生成与执行主体相关的策略，包括强制访问控制策略和级别调整策略。除此之外，安全审计员需要通过安全管理中心制定系统审计策略，实施系统的审计管理。强制访问控制机制结构如图 A-2 所示。

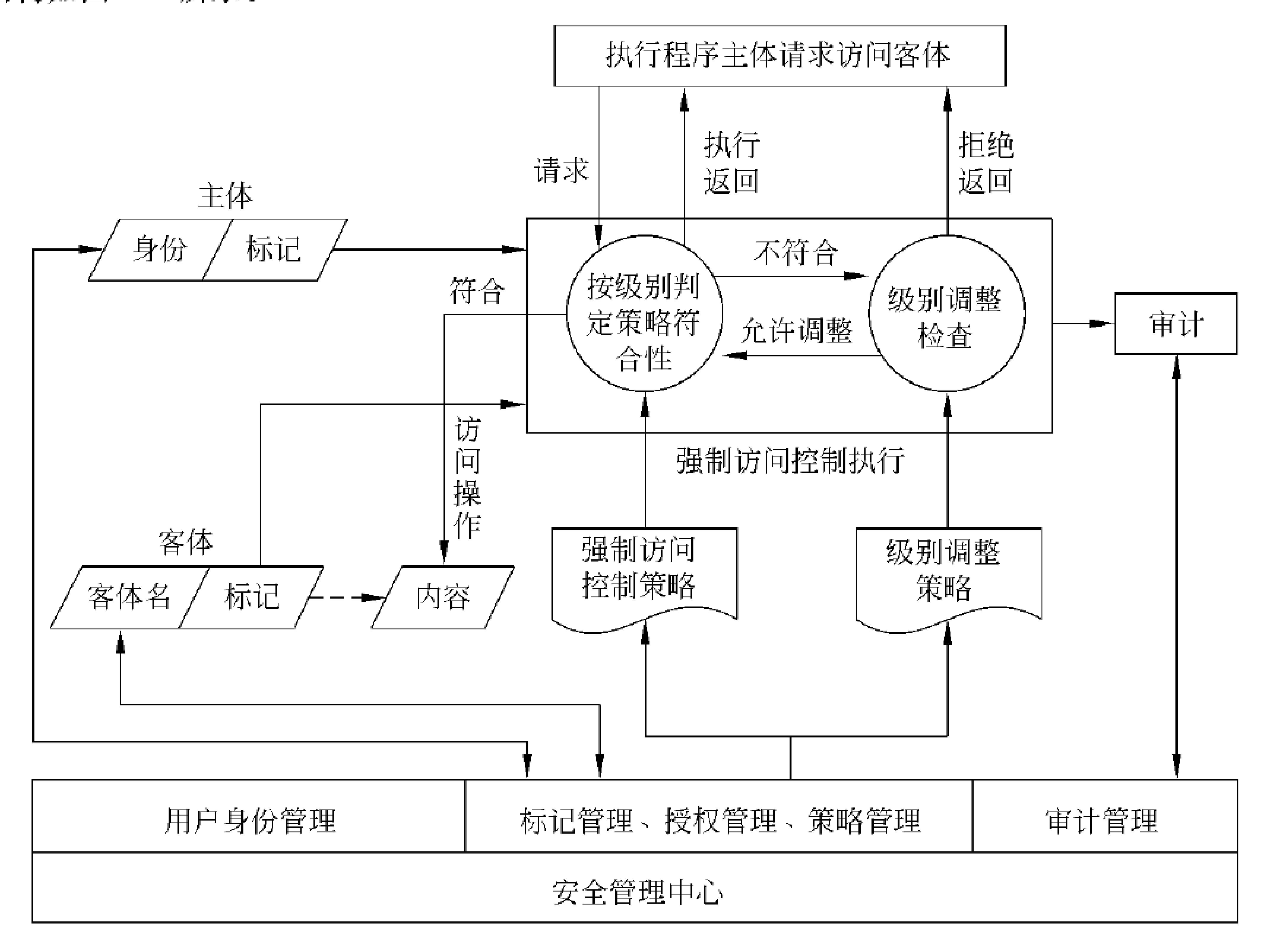



图 A-2 强制访问控制机制结构

> 系统在初始执行时，首先要求用户标识自己的身份，经过系统身份认证确认为授权主体后，系统将下载全局主/客体安全标记列表及与该主体对应的访问控制列表，并对其进行初始化。当执行程序主体发出访问系统中客体资源的请求后，系统安全机制将截获该请求，并从中取出访问控制相关的主体、客体、操作三要素信息，然后查询全局主/客体安全标记列表，得到主/客体的安全标记信息，并依据强制访问控制策略对该请求实施策略符合性检查。如果该请求符合系统强制访问控制策略，则系统将允许该主体执行资源访问。否则，系统将进行级别调整审核，即依据级别调整策略，判断发出该请求的主体是否有权访问该客体。如果上述检查通过，系统同样允许该主体执行资源访问，否则，该请求将被系统拒绝执行。
>
> 系统强制访问控制机制在执行安全策略过程中，需要根据安全审计员制定的审计策略，对用户的请求及安全决策结果进行审计，并且将生成的审计记录发送到审计服务器存储，供安全审计员管理。

**【条款解读 51】**

一、目的和意图

描述强制访问控制设计的基本方法和结构。

二、解释和示例

GB/T 24856—2009 的附录 A.2（强制访问控制机制设计），对强制访问控制机制的结构和处理流程进行了描述。

为了确保高等级信息系统的安全，在设计和实现其强制访问控制机制的过程中，必须兼顾敏感信息的保密性保护与完整性保护。然而实践证明，单纯地使保密性保护机制与完整性保护机制并存于同一信息系统会导致绝对的隔离限制，从而形成"信息孤岛"，严重降低系统可用性。因此，建立实用的、可实现的、保密性与完整性保护相结合的标记和强制访问控制工程模型是本课题研究需要解决的主要技术内容之一。

标记是实施强制访问控制的基础和依据，为正确实施强制访问控制机制，必须对信息系统中的主体和客体进行安全标记。安全标记可以采用物理绑定和逻辑绑定两种方式。物理绑定是指直接修改文件数据结构，将安全标记作为文件属性之一存储在硬盘上。逻辑绑定不对主/客体本身的数据结构进行修改，而是通过维护全局主/客体标记列表为主/客体绑定安全属性。本课题将研究基于逻辑绑定的主/客体全程标记方法。

强制访问控制的结构流程如图 A-2 所示。强制访问控制模块截获资源访问请求后，分离相关的主体、客体信息，通过查询全局主/客体标记列表，得到主/客体的安全属性。依据强制访问控制策略对该请求实施策略符合性检查。对于违反强制访问控制策略的资源访问请求，系统将进行级别调整审核。因此，还需结合应用流程研究强制访问控制策略制定方法，以及策略符合性检查和级别调整检查的实现机制。

## 1.10 第三级信息系统安全保护环境设计示例

**【标准条款】**

GB/T 24856—2009

> **附录 B（资料性附录）第三级系统安全保护环境设计示例**

**【条款解读 52】**

一、目的和意图

以资料性附录的形式，描述第三级信息系统安全保护环境设计的基本方法。

二、解释和示例

GB/T 24856—2009 的附录 B(第三级系统安全保护环境设计)，包括功能与流程、子系统间接口和重要数据结构，共三节，分别对 B.1、B.2 和 B.3 进行解释。

有关第三级信息系统安全保护环境设计的进一步解释，参见条款解读 53～条款解读 55。

## 1.10.1 功能与流程

**【标准条款】**

GB/T 24856—2009

> **B.1 功能与流程**
>
> 根据"一个中心"管理下的"三重保护"体系框架，构建安全机制和策略，形成定级系统的安全保护环境。该环境分为如下四部分：安全计算环境、安全区域边界、安全通信网络和安全管理中心。每个部分由 1 个或若干个子系统(安全保护部件)组成，子系统具有安全保护功能独立完整、调用接口简洁、与安全产品相对应和易于管理等特征。安全计算环境可细分为节点子系统和典型应用支撑子系统；安全管理中心可细分为系统管理子系统、安全管理子系统和审计子系统。以上各子系统之间的逻辑关系如图 B-1 所示。
>
> **B.1.1 各子系统的主要功能**
>
> 第三级系统安全保护环境各子系统的主要功能如下：
>
> a) 节点子系统
>
> 节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成防护层，通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，为典型应用支撑子系统的正常运行和免遭恶意破坏提供支撑和保障。
>
> b) 典型应用支撑子系统
>
> 典型应用支撑子系统是系统安全保护环境中为应用系统提供安全支撑服务的接口。通过接口平台使应用系统的主客体与保护环境的主客体相对应，达到访问控制策略实现的一致性。
>
> c) 区域边界子系统
>
> 区域边界子系统通过对进入和流出安全保护环境的信息流进行安全检查，确保不会有违反系统安全策略的信息流经过边界。
>
> d) 通信网络子系统
>
> 通信网络子系统通过对通信数据包的保密性和完整性的保护，确保其在传输过程中不会被非授权窃听和篡改，以保障数据在传输过程中的安全。
>
> e) 系统管理子系统
>
> 系统管理子系统负责对安全保护环境中的计算节点、安全区域边界、安全通信网络实施集中管理和维护，包括用户身份管理、资源管理、异常情况处理等。

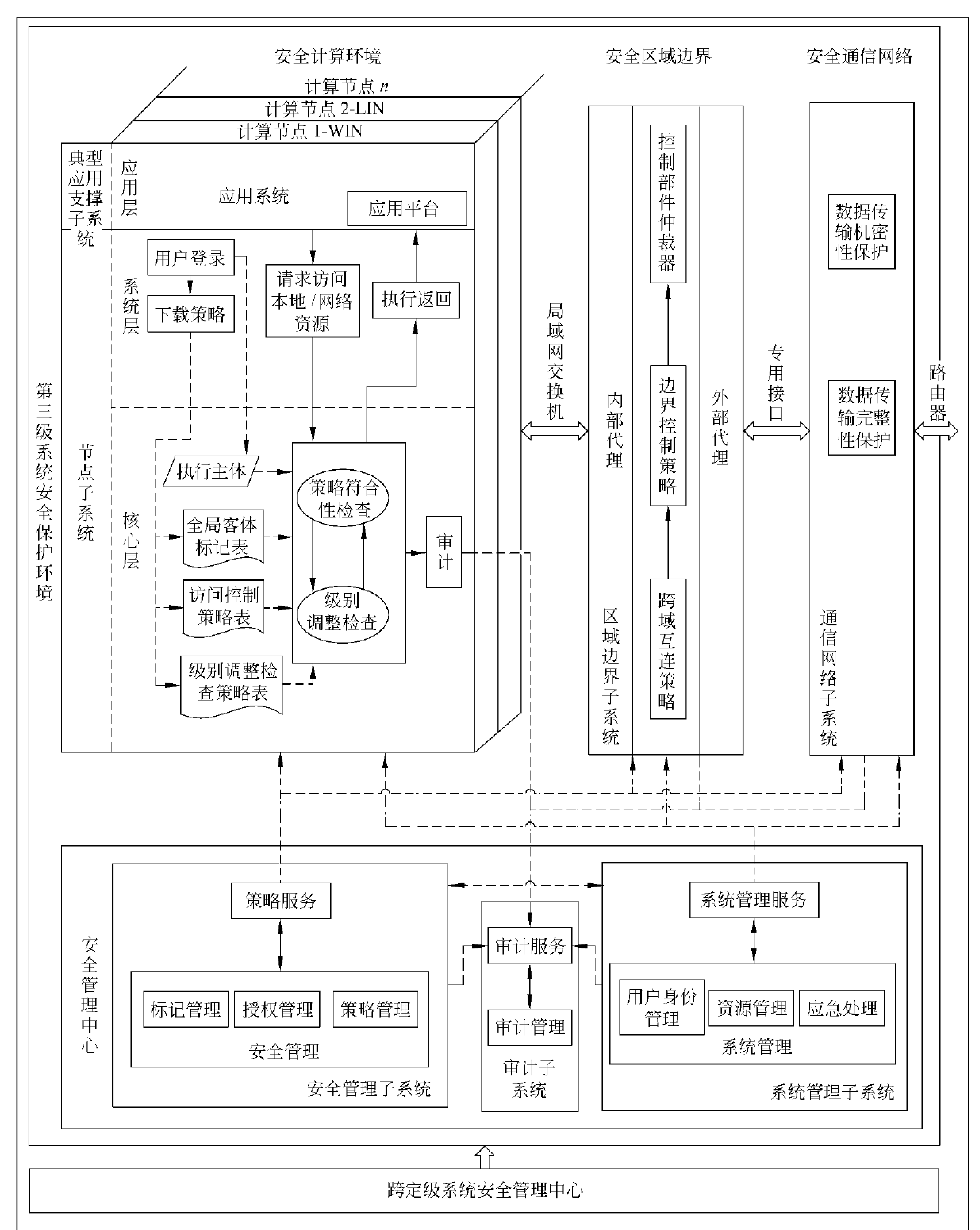



图 B-1 第三级系统安全保护环境结构与流程

f) 安全管理子系统

安全管理子系统是系统的安全控制中枢，主要实施标记管理、授权管理及策略管理等。安全管理子系统通过制定相应的系统安全策略，并要求节点子系统、区域边界子系统和通信网络子系统强制执行，从而实现对整个信息系统的集中管理。

g) 审计子系统

审计子系统是系统的监督中枢。安全审计员通过制定审计策略，并要求节点子系统、区域边界子系统、通信网络子系统、安全管理子系统、系统管理子系统强制执行，实现对整个信息系统的行为审计，确保用户无法抵赖违反系统安全策略的行为，同时为应急处理提供依据。

**B.1.2 各子系统主要流程**

第三级系统安全保护环境的结构与流程可以分为安全管理流程与访问控制流程。安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等。访问控制流程则在系统运行时执行，实施自主访问控制、强制访问控制等。

a) 策略初始化流程

节点子系统在运行之前，首先由安全管理员、系统管理员和安全审计员通过安全管理中心为其部署相应的安全策略。其中，系统管理员首先需要为定级系统中的所有用户实施身份管理，即确定所有用户的身份、工作密钥、证书等。同时需要为定级系统实施资源管理，以确定业务系统正常运行需要使用的执行程序等。安全管理员需要通过安全管理中心为定级系统中所有主、客体实施标记管理，即根据业务系统的需要，结合客体资源的重要程度，确定其安全级，生成全局客体安全标记列表。同时根据用户在业务系统中的权限和角色确定其安全标记，生成全局主体安全标记列表。在此基础上，安全管理员需要根据系统需求和安全状况，为主体实施授权管理，即授予用户访问客体资源的权限，生成强制访问控制列表和级别调整策略列表。除此之外，安全审计员需要通过安全管理中心中的审计子系统制定系统审计策略，实施系统的审核管理。如果定级系统需要和其他系统进行互联，则上述初始化流程需要结合跨定级系统安全管理中心制定的策略执行。

b) 计算节点启动流程

策略初始化完成后，授权用户才可以启动并使用计算节点访问定级系统中的客体资源。为了确保计算节点的系统完整性，节点子系统在启动时需要对所装载的可执行代码进行可信验证，确保其在可执行代码预期值列表中，并且程序完整性没有遭到破坏。计算节点启动后，用户便可以安全地登录系统。在此过程中，系统首先装载代表用户身份唯一标识的硬件令牌，然后获取其中的用户信息，进而验证登录用户是否是该节点上的授权用户。如果检查通过，系统将请求策略服务器下载与该用户相关的系统安全策略。下载成功后，系统可信计算基将确定执行主体的数据结构，并初始化用户工作空间。此后，该用户便可以通过启动应用访问定级系统中的客体资源。

c) 计算节点访问控制流程

用户启动应用形成执行主体后，执行主体将代表用户发出访问本地或网络资源的请求，该请求将被操作系统访问控制模块截获。访问控制模块首先依据自主访问控制策略对其执行策略进行符合性检查。如果自主访问控制策略的符合性检查通过，则该请求允许被执行；否则，访问控制模块依据强制访问控制策略对该请求执行策略进行符合性检查。如果强制访问策略的符合性检查通过，那么该请求允许被执行；否则，系统对其进行级别调整检查。即依照级别调整检查策略，判断发出该请求的主体是否有权访问该客体。如果通过，该请求同样允许被执行；否则，该请求被拒绝执行。

系统访问控制机制在安全决策过程中，需要根据安全审计员制定的审计策略，对用户的请求及决策结果进行审计，并且将生成的审计记录发送到审计服务器存储，供安全审计员检查和处理。

d) 跨计算节点访问控制流程

如果主体和其所请求访问的客体资源不在同一个计算节点，则该请求会被可信接入模块截获，用来判断该请求是否会破坏系统安全。在进行接入检查前，模块首先通知系统安全代理获取对方

计算节点的身份，并检验其安全性。如果检验结果是不安全的，则系统拒绝该请求；否则，系统将依据强制访问控制策略，判断该主体是否允许访问相应端口。如果检查通过，该请求被放行；否则，该请求被拒绝。

e) 跨边界访问控制流程

如果主体和其所请求访问的客体资源不在同一个安全保护环境内，那么该请求将会被区域边界控制设备截获并且进行安全性检查，检查过程类似于跨计算节点访问控制流程。

**【条款解读 53】**

一、目的和意图

描述第三级信息系统安全保护环境各子系统的功能与流程。

二、解释和示例

GB/T 24856—2009 的附录 B.1（功能与流程），从各子系统的主要功能、各子系统的主要流程等方面，对第三级信息系统安全保护环境各子系统的功能与流程进行说明。对第三级信息系统安全保护环境各子系统主要功能的描述包括：节点子系统的功能描述，典型应用子系统的功能描述，区域边界子系统的功能描述，通信网络子系统的功能描述，系统管理子系统的功能描述，安全管理子系统的功能描述，以及审计子系统的功能描述。对第三级信息系统安全保护环境各主要处理流程的描述包括：策略初始化流程的描述，计算节点启动流程的描述，计算节点访问控制流程的描述，跨节点控制流程的描述，以及跨边界访问控制流程的描述。其中所谓节点子系统即为计算节点所构成的子系统。

## 1.10.2 子系统间的接口

**【标准条款】**

GB/T 24856—2009

**B.2 子系统间的接口**

**B.2.1 综述**

为了清楚描述各子系统之间的关系，图 B-2 给出了子系统间的接口关系。

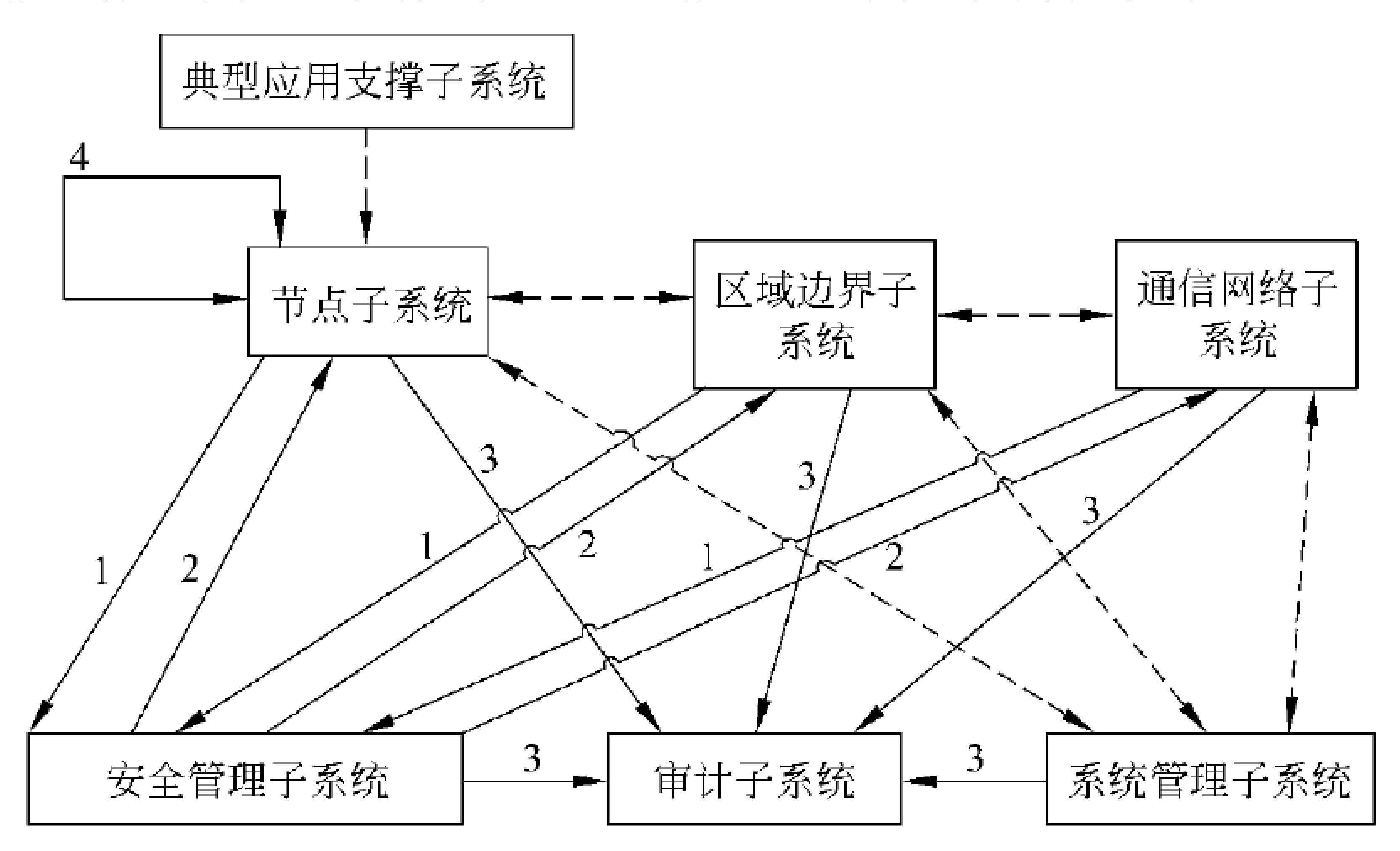



图 B-2 第三级系统安全保护环境子系统接口

典型应用支撑子系统与节点子系统之间通过系统调用接口。其他子系统之间则通过可靠的网络传输协议,按照规定的接口协议传输策略数据、审计数据以及其他安全保护环境数据等。由于不同子系统之间需要交换各种类型的数据包,因此需要明确定义子系统间的接口协议并规范传输数据包格式,使得各子系统之间能透明交互,实现相应数据的交换。数据包的标准格式见表 B-1。

**表 B-1 子系统间数据包格式**

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 标志 | | | | 版本号 | | | | 接口类型 | | | | 标记位 | | | |
| 内容长度 | | | | 附加项长度 | | | | 保留 | | | | | | | |
| 数据内容 | | | | | | | | | | | | | | | |
| …… | | | | | | | | | | | | | | | |
| 附加项类型 | | | | 附加项内容 | | | | | | | | | | | |
| …… | | | | | | | | | | | | | | | |

数据包由包头、附加项和数据内容三部分组成,其中包头为 32 字节,定义了标志、版本号、接口类型、标记位以及内容和附加项长度等。内容和附加项长度不定。

数据包各数据项说明如下:

标志(4 字节):用于标识等级保护相关的数据流,此标志可以作为区别等级保护数据包的依据。

版本号(4 字节):表示该接口协议的版本号。其中前两个字节表示主版本号。

接口类型(4 字节):表示本数据包的对应接口类型编号。

标记位 (4 字节):表述数据包属性标志,见表 B-2。

**表 B-2 数据包属性标志**

| 保留(29 比特位) | BRO | SIG | CHK |
|---|---|---|---|

BRO:表示数据包发送对象地址尚未确定,需要以广播方式发送或发送给查询服务器。

SIG:表示数据包是否有签名保护,0 为无签名,1 为有签名。如果有签名保护,签名信息在附加项中显示。

CHK:表示数据包是否需要校验,0 为不校验,1 为校验。如果需要校验,校验码在附加项中存放。

内容长度(4 字节):表示数据包内容的部分长度,以字节为单位。

附加项长度(4 字节):表示所有附加项长度之和,以字节为单位。

保留(8 字节):作为数据包扩展保留。

数据内容:数据包传输的具体内容,其格式与数据包类型相关,长度不定。

附加项类型(4 字节):表示附加项的类型。

附加项内容:数据包传输的附加内容,其格式与附加项类型相关,长度不定。

下面按照接口对应的数据包类型介绍数据内容部分,表格中不含包头和附加项。

**B.2.2 接口 1**

功能:节点(区域边界、通信网络)子系统向安全管理子系统请求下载策略。

类型：请求数据包。

描述：计算节点、区域边界、通信网络设备启动时，向安全管理子系统请求下载策略，该接口为节点子系统、区域边界子系统、通信网络子系统到安全管理子系统之间的接口。

客户端向服务器发起 TCP 连接，发出的请求数据包数据内容格式见表 B-3。

**表 B-3 客户端向服务器发出的请求数据包数据内容格式**

<table>
<tr><td colspan="3">节点标志(1～16 字节)</td></tr>
<tr><td>节点标志(17～20 字节)</td><td colspan="2">用户身份(1～12 字节)</td></tr>
<tr><td colspan="3">用户身份(13～28 字节)</td></tr>
<tr><td colspan="2">用户身份(29～40 字节)</td><td>附加信息长度</td></tr>
<tr><td colspan="3">附加信息</td></tr>
<tr><td colspan="3">……</td></tr>
</table>

**B.2.3 接口 2**

功能：安全管理子系统向节点(区域边界、通信网络)子系统返回与请求主体相关的策略。

类型：策略下发数据包。

描述：安全管理中心接到下载策略请求后，向计算节点、区域边界、通信网络设备发送安全策略。

安全管理子系统策略下发数据包数据内容格式见表 B-4。

**表 B-4 安全管理子系统策略下发数据包数据内容格式**

<table>
<tr><td colspan="4">节点标志(1～16 字节)</td></tr>
<tr><td>节点标志(17～20 字节)</td><td colspan="3">用户身份(1～12 字节)</td></tr>
<tr><td colspan="4">用户身份(13～28 字节)</td></tr>
<tr><td colspan="3">用户身份(29～40 字节)</td><td>策略类型</td></tr>
<tr><td colspan="2">策略版本(8 字节)</td><td>策略项数(4 字节)</td><td>保留(4 字节)</td></tr>
<tr><td colspan="4">下载策略项 1</td></tr>
<tr><td colspan="4">……</td></tr>
<tr><td colspan="4">下载策略项 2</td></tr>
<tr><td colspan="4">……</td></tr>
</table>

**B.2.4 接口 3**

功能：节点(区域边界、通信网络)子系统向审计服务器发送审计记录。

类型：审计记录数据包的数据内容格式。

描述：计算节点、区域边界、通信网络设备向审计子系统发送审计记录。

所发送的审计记录数据包数据内容格式见表 B-5。

表 B-5 节点子系统发送的审计记录数据包的数据内容格式

| | | |
|---|---|---|
| 节点标志(1～16 字节) | | |
| 节点标志(17～20 字节) | 审计项数(4 字节) | 保留 |
| 第 1 个审计项 | | |
| …… | | |
| 第 2 个审计项 | | |
| …… | | |
| 第 n 个审计项 | | |
| …… | | |

**B.2.5 接口 4**

功能：节点子系统之间的接入可信性验证。

类型：可信接入申请包、可信接入应答包、可信接入确认包。

描述：节点子系统之间的接口主要实现可信接入。可信接入是在执行跨节点间访问时，客体所在节点验证主体所在节点可信性的过程。可信接入需要三步协议执行。首先是访问发起方所在节点向访问应答方所在节点提出可信接入申请包，应答方所在节点验证申请包后向发起方所在节点发送可信接入应答包，由发起方所在节点验证应答包成功后，返回可信接入确认包。

可信接入申请包格式见表 B-6。

表 B-6 可信接入申请包数据内容格式

| | |
|---|---|
| 发起方平台身份(1～16 字节) | |
| 发起方平台身份(17～32 字节) | |
| 附加项长度(4 字节) | 附加项 |

可信接入应答包格式见表 B-7。

表 B-7 可信接入应答包数据内容格式

| | |
|---|---|
| 应答方平台身份(1～16 字节) | |
| 应答方平台身份(17～32 字节) | |
| 附加项长度(4 字节) | 附加项 |

可信接入确认包数据内容格式和可信接入应答包内容格式相同，具体区别在于附加项。

**【条款解读 54】**

一、目的和意图

描述第三级信息系统安全环境设计各子系统间的接口。

二、解释和示例

GB/T 24856—2009 的附录 B.2，首先以图 B-2 的形式，对第三级系统安全保护环境子系统接口进行了总体描述，然后分别对接口 1：节点(区域边界、通信网络)子系统

——>安全管理子系统，接口 2：安全管理子系统——>节点(区域边界、通信网络)子系统，接口 3：节点(区域边界、通信网络)子系统——>审计子系统，以及接口 4：节点子系统——>节点子系统等各接口的具体实现进行了比较详细的说明。

## 1.10.3 重要数据结构

**【标准条款】**

GB/T 24856—2009

**B.3 重要数据结构**

**B.3.1 重要数据结构列表**

第三级系统安全保护环境设计的重要数据结构见表 B-8。

**表 B-8 重要数据结构**

| 编号 | 数据结构名称 | 用途 |
|---|---|---|
| 1 | 用户身份信息列表 | 用户身份、密钥等信息列表 |
| 2 | 主体安全标记列表 | 以此表为依据，可以利用用户身份查询其标记信息 |
| 3 | 客体安全标记列表 | 以此表为依据，可以利用客体名查询其标记信息 |
| 4 | 自主访问控制列表 | 确定了主体能自主访问的客体 |
| 5 | 级别调整策略列表 | 确定了主体能特权操作的客体 |
| 6 | 审计策略列表 | 确定了系统的审计策略，即需要对哪些安全事件进行审计 |
| 7 | 审计记录格式 | 审计日志 |

**B.3.2 用户身份信息列表**

```
typedef struct tagUser_Info
{
    BYTE * RootCert;
    UINT32 RootCertLen;
    BYTE * UserCert;
    UINT32 UserCertLen;
    BYTE * UserSigKey;
    UINT32 UserSigKeyLen;
    BYTE EncAlgID;
    BYTE * WorkKey;
    UINT32 WorkKeyLen;
    BYTE * UserEncKey;
    UINT32 UserEncKeyLen;
    BYTE Reserved[256];
} User_Info;
```

用户身份信息列表字段解释见表 B-9。

表 B-9 重要数据结构

| 字段名 | 解　　释 | 字段名 | 解　　释 |
| --- | --- | --- | --- |
| RootCert | 系统根证书 | EncAlgID | 对称加密算法标识 |
| RootCertLen | 系统根证书长度 | WorkKey | 全系统统一的对称加密密钥 |
| UserCert | 用户证书 | WorkKeyLen | 全系统统一的对称加密密钥长度 |
| UserCertLen | 用户证书长度 | UserEncKey | 用户私有对称加密密钥 |
| UserSigKey | 用户签名私钥 | UserEncKeyLen | 用户私有对称加密密钥长度 |
| UserSigKeyLen | 用户签名私钥长度 | Reserved | 保留字段 |

### B.3.3 主体安全标记列表

```
typedef struct SubjectLabel
{
    UINT32 SubNameLength;
    BYTE * sSubName;
    UINT32 GroupNameLength;
    BYTE * sGroupName;
    BYTE  ConfLevel;
    BYTE  InteLevel;
    BYTE  SecClass[8];
    BYTE  SubType;
}Sub_Label;
```

主体安全标记列表字段解释见表 B-10。

表 B-10 主体安全标记列表字段

| 字段名 | 解　　释 |
| --- | --- |
| SubNameLength | 主体名长度 |
| sSubName | 主体名 |
| GroupNameLength | 主体所属组名称长度 |
| sGroupName | 主体所属组名称 |
| ConfLevel | 用于标识主体的保密性级别 |
| InteLevel | 用于标识主体的完整性级别 |
| SecClass | 表示主体所属的范畴，共 64 位，8 位标识一个范畴，总共可以标识 8 个范畴，从高位到低位范畴级别依次降低。 |
| SubType | 表示主体类型，即主体是否是安全管理员、系统管理员、安全审计员、普通操作员、进程或设备。 |

### B.3.4　客体安全标记列表

```
typedef struct ObjectLabel
{
    UINT32 ObjNameLength;
    BYTE * sObjName;
    BYTE   ConfLevel;
    BYTE   InteLevel;
    BYTE   SecClass[8];
    BYTE   ObjType;
}Obj_Label;
```

客体安全标记列表字段解释见表 B-11。

**表 B-11　客体安全标记列表字段**

| 字段名 | 解　　释 |
|---|---|
| ObjNameLength | 客体名长度 |
| sObjName | 客体名称 |
| ConfLevel | 用于标识客体的保密性级别 |
| InteLevel | 用于标识客体的完整性级别 |
| SecClass | 表示客体所属的范畴，共 64 位，8 位标识一个范畴，总共可以标识 8 个范畴，从高位到低位范畴级别依次降低。 |
| ObjType | 表示客体类型，即客体是否是系统文件、审计文件、策略文件、业务文件、系统服务或设备文件，以及客体是否需要加密保护。 |

### B.3.5　自主访问控制列表

```
typedef struct DAC_List
{
    UINT32 SubNameLength;
    BYTE * sSubName;
    UINT32 ObjNameLength;
    BYTE * sObjName;
    BYTE   OperateType;
}DAC_Label;
```

自主访问控制列表字段解释见表 B-12。

**表 B-12　自主访问控制列表字段**

| 字段名 | 解　　释 |
|---|---|
| SubNameLength | 主体名长度 |
| sSubName | 主体名或主体组名 |
| ObjNameLength | 客体名长度 |
| sObjName | 客体名 |
| OperateType | 操作类型，包括创建、打开、读、写、修改、执行、更名和删除等 |

**B.3.6 级别调整策略列表**

```
typedef struct tagPriviledge_List
{
    UINT32 SubNameLength;
    BYTE * sSubName;
    UINT32 ObjNameLength;
    BYTE * sObjName;
    BYTE  OperateType;
    UINT32 AuthOwnerNameLength;
    BYTE * sAuthOwnerName;
}PRIV_Label;
```

级别调整策略列表字段解释见表 B-13。

**表 B-13 级别调整策略列表字段**

| 字 段 名 | 解 释 |
|---|---|
| SubNameLength | 主体名长度 |
| sSubName | 主体名或主体所属组名 |
| ObjNameLength | 客体名长度 |
| sObjName | 客体名 |
| OperateType | 操作类型,包括创建、打开、读、写、修改、执行、更名和删除等。 |
| AuthOwnerNameLength | 授权者用户名长度 |
| sAuthOwnerName | 授权者用户名 |

**B.3.7 审计策略列表**

```
typedef struct auditpolicytime
{
    BYTE  Year[4];
    BYTE  Month[2];
    BYTE  Day[2];
    BYTE  Hour[2];
    BYTE  Min[2];
    BYTE  Sec[2];
    BYTE  Week[2];
}APTIME;
typedef struct tagAUDIT_POLICY_TERM
{
    UINT16  NodeID;
    UINT16  iType;
    UINT16  Bret;
```

```
    SHORT  IsOn;
    APTIME  BeginTime;
    APTIME  EndTime;
    UINT32  Reserved;
} AUDIT_POLICY_TERM, * PAUDIT_POLICY_TERM;
```

审计策略列表字段解释见表 B-14。

**表 B-14 审计策略列表字段**

| 字段名 | 解　　释 |
|---|---|
| NodeID | 节点的 ID 号 |
| iType | 审计事件类型、类别 |
| Bret | 共两个字节，第一个字节表示动作行为，第二个字节表示动作结果及其原因 |
| IsOn | 审计开关 0：off；1：on |
| BeginTime | 审计开始时间 |
| EndTime | 审计结束时间 |
| Reserved | 保留字段 |

### B.3.8 审计记录

```
typedef struct audit_label
{
    BYTE  Name[21];
    BYTE  ConfLevel;
    BYTE  InteLevel;
    BYTE  SecClass[8];
    BYTE  Type;
}ALABEL, * PALABEL;
typedef struct tagAudit_Record
{
    UINT16  NodeID;
    UINT16  iType;
    UINT32  Time;
    ALABEL  SubLabel;
    ALABEL  ObjLabel;
    UINT16  Bret;
    Byte    Reserved[6];
}Audit_Record;
```

审计记录字段解释见表 B-15。

表 B-15 审计记录字段

| 字段名 | 解 释 |
|---|---|
| NodeID | 事件节点编号 |
| iType | 事件类型，包括身份鉴别、客体访问或用户行为等 |
| Time | 事件发生时间 |
| SubLabel | 事件发起主体安全标记 |
| ObjLabel | 事件对应客体安全标记 |
| Bret | 事件的操作行为、结果及其原因 |
| Reserved | 保留字段 |

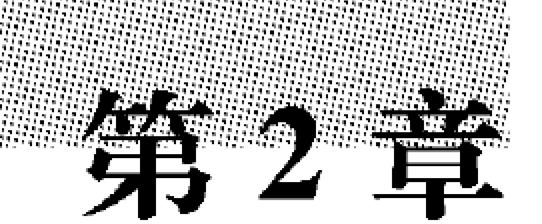
**【条款解读 55】**

一、目的和意图

描述第三级信息系统安全环境设计的重要数据结构。

二、解释和示例

GB/T 24856—2009 的附录 B.3(重要数据结构)，分别对用户身份信息列表、主体安全标记列表、客体安全标记列表、自主访问控制列表、审计策略列表、审计数据格式等重要数据进行了描述。



# 第2章 二级信息系统安全设计和实现

## 2.1 安全功能和总体结构

二级信息系统的总体结构如图 2-1 所示。

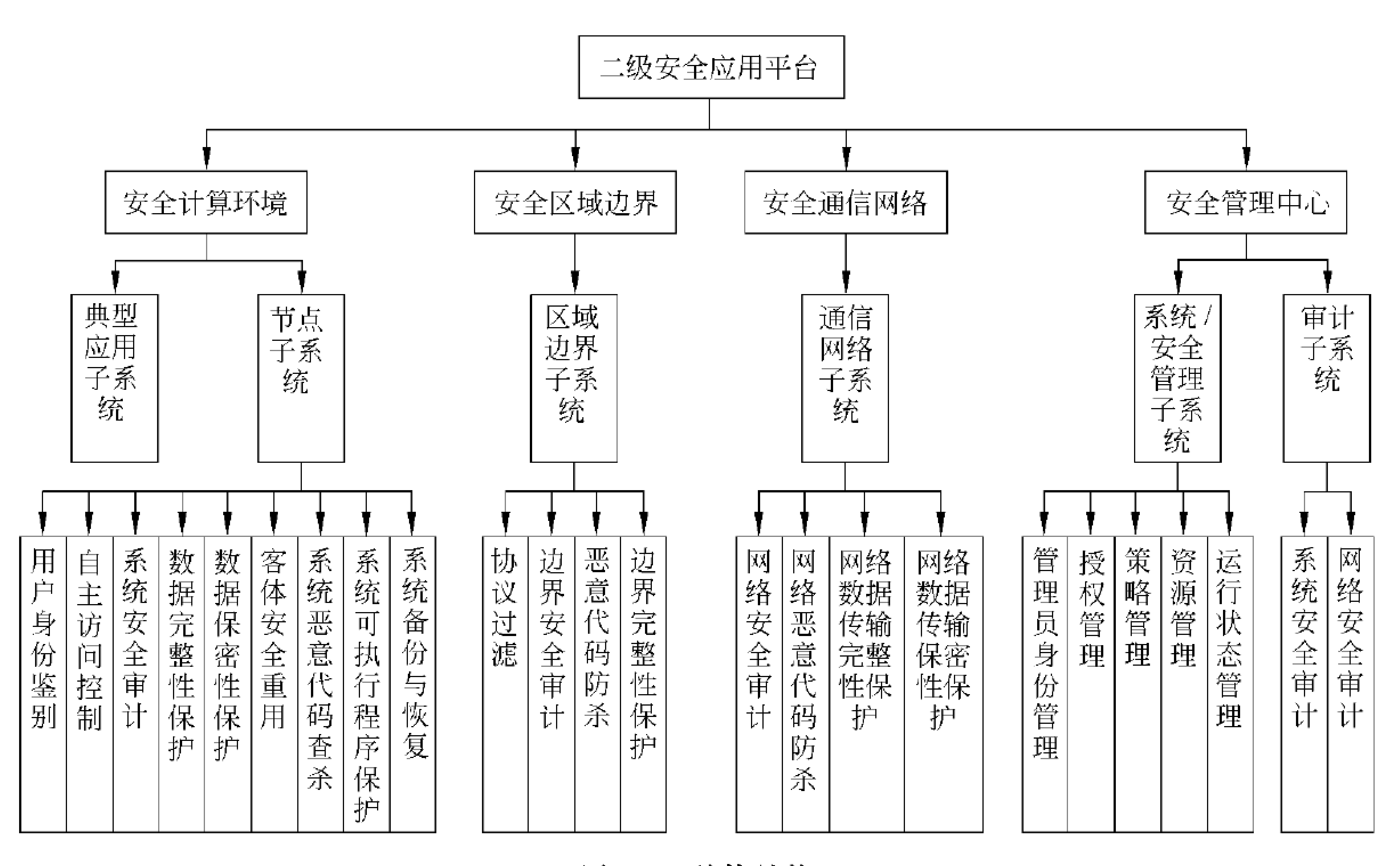



图 2-1　总体结构

### 1. 信息系统实现功能

落实 GB 17859—1999 的 4.2 关于“通过登录规则、审计安全性相关事件和隔离资源，使用户对自己的行为负责”的要求，实现第二级系统安全保护环境，以提供系统审计安全保护的基础。增加对安全相关事件的审计机制，将自主访问控制的粒度增加到单个用户，使用户行为具有可查性，并以用户身份鉴别、存储、传输和处理过程中用户数据的完整性、保密性、可用性保护以及对客体安全重用的支持等，共同实现数据保护的安全。同时，通过较高要求的安全运行控制，确保安全应用平台为应用软件系统的安全运行提供较好的支持，实现提供可靠服务的安全性。

### 2. 一个中心管理下的三重防御体系

为已定级信息系统构建安全保护环境，是以较低成本实现其安全保护能力的合理方式，具有技术上成熟、产品选择面宽、无需对业务系统进行修改的优点。

安全保护环境的核心在于构建"一个中心"管理下的"三重防御体系"。"一个中心"是指安全管理中心，包括系统管理、安全管理和审计管理。"三重防御体系"包括提供安全计算环境、提供安全区域边界和提供安全通信网络。安全计算环境可细分为：节点子系统和典型应用子系统；安全管理中心分为系统管理子系统、安全管理子系统和审计子系统。二级系统安全保护环境的体系结构如图 2-2 所示。

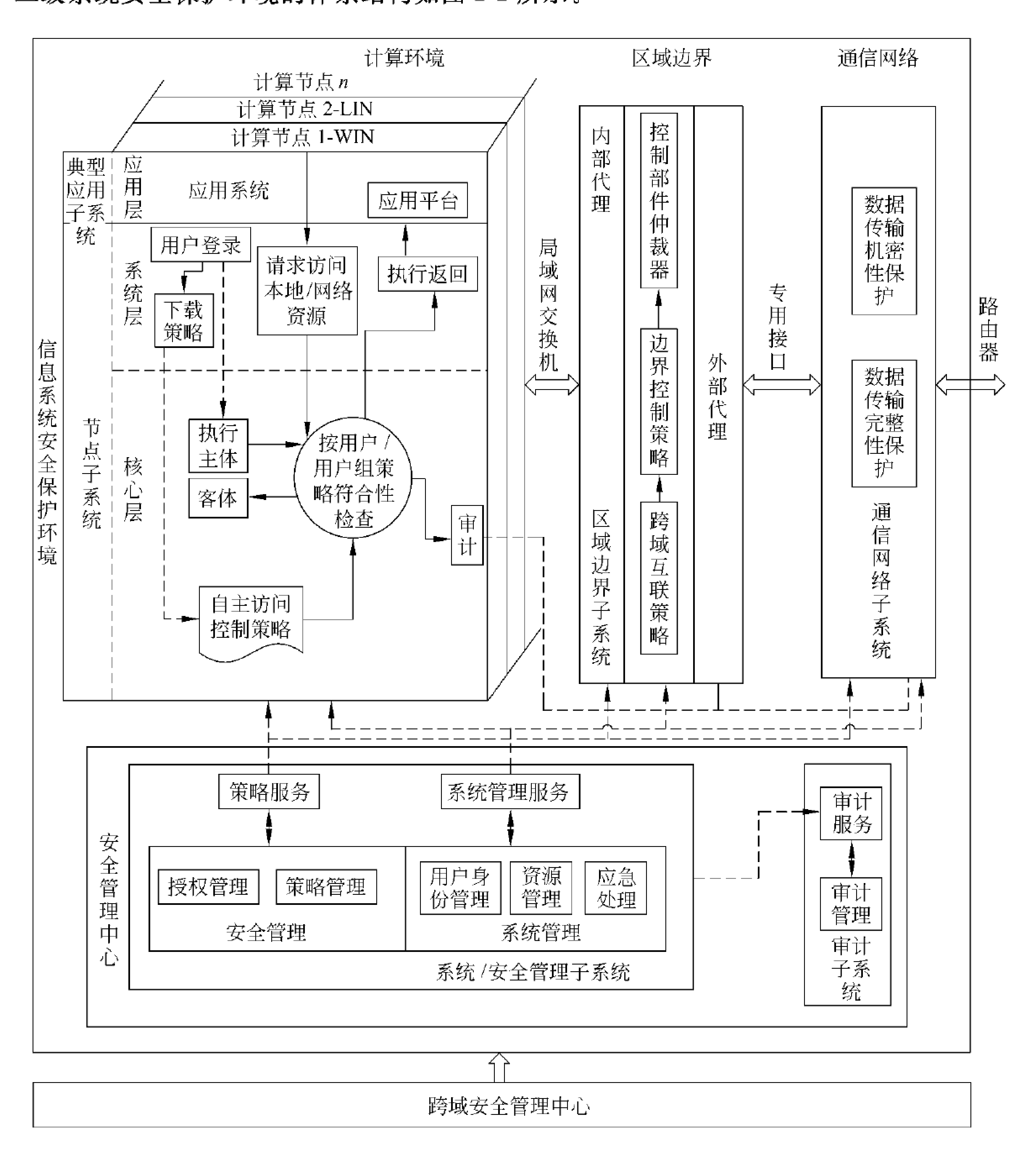



图 2-2　二级系统安全保护环境体系结构

# 2.2 实现方案和设备类型

## 2.2.1 安全计算环境建设

进行第二级安全计算环境建设的重点在于进行系统加固，实现用户身份鉴别、自主访问控制、实现系统安全审计、实现客体重用并且提供恶意代码防范的功能。

参照上述第二级系统安全保护环境的安全计算环境的安全技术要素，实现安全计算环境的安全功能，需安装如下几个软件系统。

### 1. 部署二级操作系统

进行操作系统加固不仅需要对服务器的操作系统进行加固，并且需要对用户操作终端计算机进行系统加固。

### 2. 部署系统安全审计系统

安全计算环境的系统安全审计主要是对服务器、安全终端的系统安全事件进行审计。在本方案中通过在各服务器以及安全终端部署系统安全审计探头，对重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用等记录的日期和时间、用户、事件类型、事件是否成功等进行记录，并可以将这些记录转换为标准格式，通过审计代理将审计记录提交给审计管理中心。

### 3. 部署客体重用系统

进行剩余信息保护，主要在于对使用的客体资源进行监控和管理。在本方案中通过部署客体重用系统，在该客体资源重新分配前对其原使用者的信息进行清除，以确保系统的重要信息不被泄露。

### 4. 部署防病毒软件

综合考虑安全计算环境对恶意病毒查杀的安全功能要求。在本方案中选用瑞星杀毒软件网络版。通过此病毒防护系统提供的系统管理中心、管理员控制台、杀毒软件服务器端、客户端，为安全计算环境建立全方位的病毒防护体系。并且可以实现远程管理、智能升级、自动分发、远程报警等多种功能。

## 2.2.2 安全通信网络建设

在第二级系统安全保护环境中的安全网络建设主要用于实现网络安全审计，并依据客户实际应用的要求为用户的网络数据传输提供完整性和保密性保护。

参照上述第二级系统安全保护环境的安全通信网络的安全技术要素，实现安全通信网络的安全功能，需安装如下几个软件系统。

### 1. 部署网络安全审计系统

在本方案中通过部署网络行为审计系统，对用户行为进行探测、收集、还原，并且可以

对其他网络设备日志、其他审计产品日志进行获取，实现对安全通信网络中所有的网络安全事件的集中存储、管理和分析。

**2. 建立 IPSEC VPN**

网络数据传输完整性、保密性保护主要体现在与两个安全计算环境之间的网络数据传输的完整性和保密性保护。在本方案中通过在两个安全计算环境间建立 IPSEC VPN，通过 IPSEC VPN 提供的数据校验机制以及加密机制，为网络数据传输提供完整性和保密性保护。

### 2.2.3 安全区域边界建设

在第二级系统安全保护环境中的安全区域边界建设主要在于实现区域边界协议过滤、区域边界安全审计、区域边界恶意代码防范、区域边界完整性保护等安全功能。

参照上述第二级系统安全保护环境的安全区域边界的安全技术要素，实现安全区域边界的安全功能，需安装如下几个软件系统。

**1. 部署防火墙**

在本方案中通过部署安置防火墙，实现以下几个安全要素。

(1) 状态检测和访问控制

采用基于状态检测的包过滤技术，快速实现基于源/目的 IP 地址、源 MAC 地址、服务/端口、用户、时间、组(网络、服务、用户、时间)的精细粒度的访问控制。

(2) 内容过滤

http 关键字、命令过滤 、文件名过滤 、URL 过滤 、邮件关键字过滤、邮件文件名过滤、发件人邮箱过滤、收件人邮箱过滤、http 命令过滤(get、put、post)、Java scripts/Active-X 过滤封堵、Java 小程序控制、Cookie 过滤、http、smtp、pop3、ftp、telnet 等协议的内容过滤。

(3) 透明应用代理

提供丰富全面的应用代理，覆盖大多数用户常用应用程序，包括 HTTP、SMTP、POP3、FTP、TELNET 代理等。同时，多线程的代理提供较高性能的连接速度。提供多种内核级别代理机制，例如 FTP、TFTP 和 ICMP 代理可极大增强特殊网络应用安全性。

(4) 网络地址转换

① 支持多种方式的网络地址转换，包括：静态地址映射、静态地址转换(1∶1)、动态地址转换(N∶1,N∶N)、反向 NAT；

② DMZ 区的特殊地址转换，即端口转换能力，加强 DMZ 区的安全保护；

③ 负载均衡。

(5) 日志、审计和告警

防火墙提供五种日志内容：连接日志、攻击日志、代理日志、认证日志和配置日志。并且可以对任意的日志内容、任意级别指定不同的日志报警方式。系统提供的告警方式包括：声音报警、邮件通知、Windows 消息、用户终端、系统缓冲区，支持日志的本地存储、远端存储、备份等存储方式。

### 2. 部署可信接入网关

对接入网络的计算机终端实施强制平台身份认证，检查计算机终端安全状态，阻断非受控终端以及不符合安全策略的终端接入网络。并且提供终端接入审计、访问控制、系统日志。

### 3. 部署入侵检测系统

在安全区域边界中，部署入侵检测系统，检测并记录 attack-responses、backdoor、chat、ddos、dns、dos、exploit、finger、ftp、icmp、misc、multimedia、netbios、oracle、p2p、policy、pop3、rpc、rservices、scan、shellcode、smtp、snmp、sql、telnet、tftp、virus、web-attacks、web-cgi、web-client、web-coldfusion、web-frontpage、web-iis、web-misc、web-php 等攻击行为。

## 2.2.4 安全管理中心建设

安全管理中心的安全功能基本结构如图 2-3 所示。

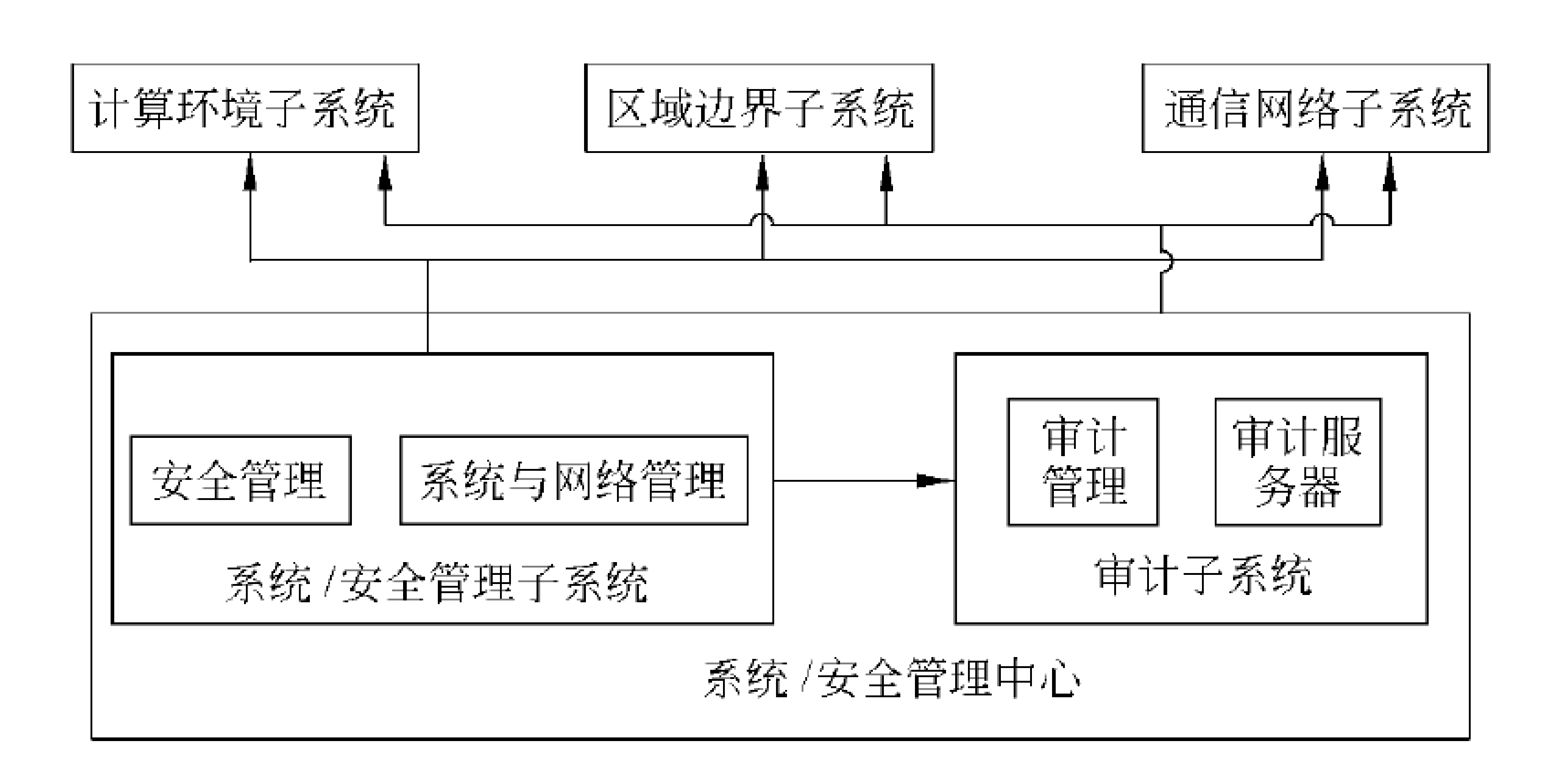



图 2-3 安全管理中心的安全功能基本结构

建立安全管理中心的目标在于实现对在进行安全保护环境建设过程中所部属的各系统进行集中管理。在第二级安全管理中心主要需要部署自主访问控制管理中心，系统安全审计管理中心，病毒防护管理中心和网络资源管理中心。

### 1. 部署自主访问控制系统管理中心

管理员通过控制台对整个系统的安全策略进行配置与控制。从该控制台登录并管理系统的有下面三类管理员。

(1) 系统管理

系统管理子系统用于对节点子系统、区域边界子系统、通信网络子系统的软硬件进行管理和维护，发行用户硬件令牌，对系统异常行为作应急处理。

(2) 安全管理

安全管理子系统策略配置包括：主/客体标记案例管理、用户授权管理、策略管理等。

(3) 审计管理

审计子系统用于存储和处理整个系统中的所有审计信息。节点子系统、区域边界子

系统、通信网络子系统和安全管理子系统、系统管理子系统等获得审计信息后形成文件，上传到审计服务器进行存储和处理。

**2. 部署安全审计管理中心**

实现对计算环境内各节点上的主机安全审计信息、自主访问控制审计信息、客体重用审计信息以及对边界安全设备的审计信息的统一集中管理。

### 2.2.5　系统安全互联

**1. 安全互联部件设计技术的要求**

安全互联部件是通信网络交换网关，与各定级系统安全保护环境的安全通信网络部件相连接，按互联互通的安全策略进行信息交换。安全策略由跨定级系统的安全管理中心实施。

**2. 建立跨定级系统安全管理中心**

跨定级系统安全管理中心通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的系统管理、安全管理和审计管理。

(1) 系统管理

应通过系统管理员对安全互联部件与相同和不同等级的定级系统中与安全互联相关的系统资源和运行进行配置和管理，包括用户身份管理、安全互联部件资源配置和管理等。

(2) 安全管理

应通过安全管理员对相同和不同等级的定级系统中与安全互联相关的主/客体进行标记管理，使得其标记信息能够准确反映主/客体在定级系统中的安全属性；对主体进行授权，配置统一的安全策略，并确保授权信息在相同和不同等级的定级系统中的合理性。

(3) 审计管理

应通过安全审计员对安全互联部件的安全审计机制和各定级系统跨定级系统互联有关的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对审计记录进行分析，并根据分析结果进行及时处理。

## 2.3　安全计算环境子系统的设计和实现

计算环境子系统是在操作系统自带的功能基础上进行扩展，加入身份认证模块，访问控制模块，安全重用模块和数据完整性模块，如图 2-4 所示。

下面对各组成结构总模块进行几点说明。

① 身份认证模块：通过标识和鉴别确保用户与正确的安全属性相关联(如身份、组、角色、安全或完整性等级)。

② 访问控制模块：确定访问控制策略及其控制范围，执行自主访问控制机制。

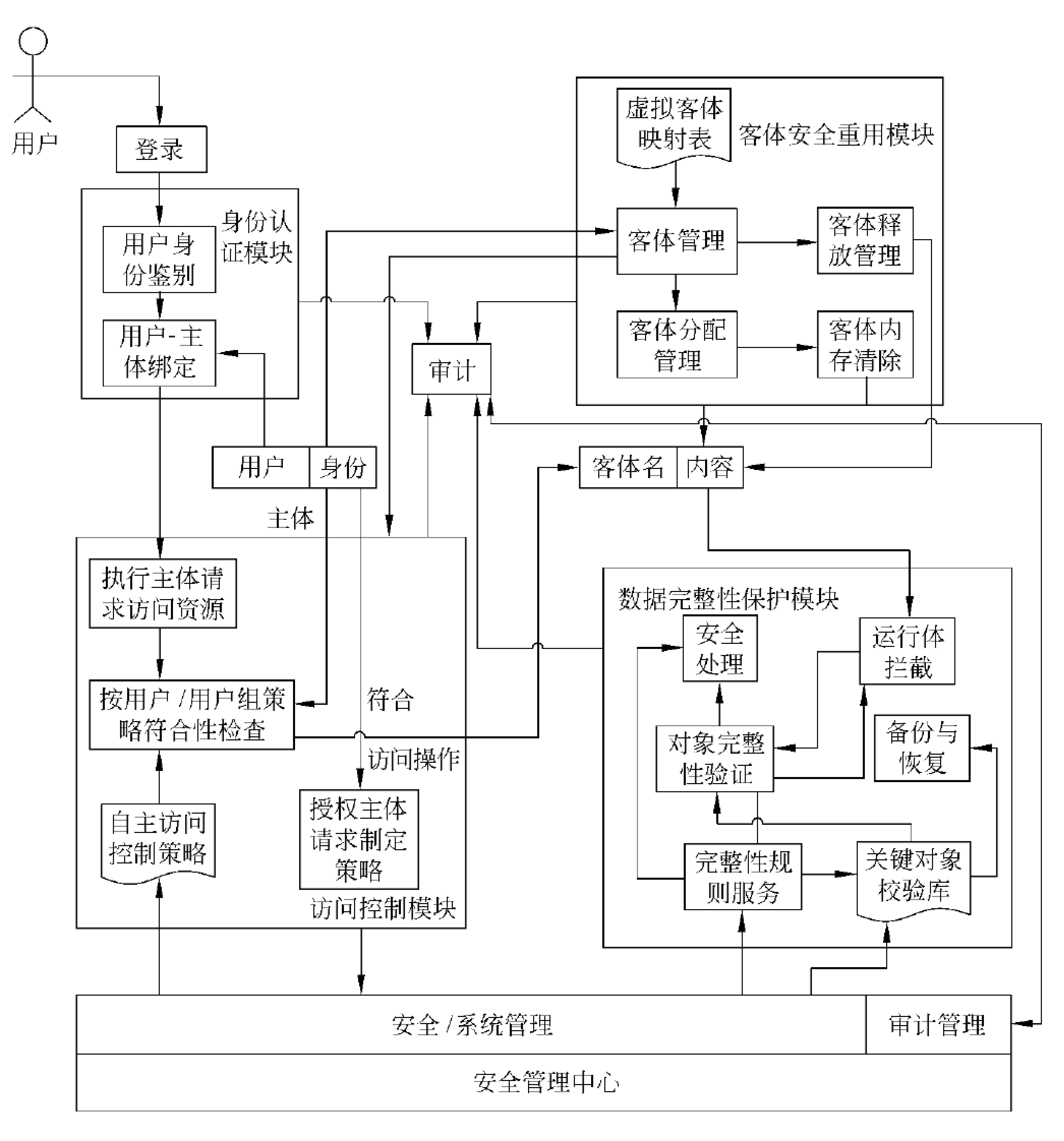



图 2-4 计算环境子系统基本结构

③ 数据完整性模块：对存储数据的完整性进行监视，在检测到某错误时，采取相应的行动。

④ 客体安全重用模块：在将文件和内存分配给一个用户之前，先对它们进行初始化。

⑤ 审计：识别、记录、存储和分析那些与安全相关活动有关的信息。检查审计记录结果可用来判断发生了哪些安全相关活动以及哪个用户要对这些活动负责。

## 2.3.1 身份认证模块结构

身份认证模块的结构如图 2-5 所示。

### 1. 用户标识

用户在执行任何其他由评估对象的安全功能促成的有用户标识的行动之前，应先标识他们自己。如果允许用户在被标识之前执行某些行动，必须提供对行动的管理列表。

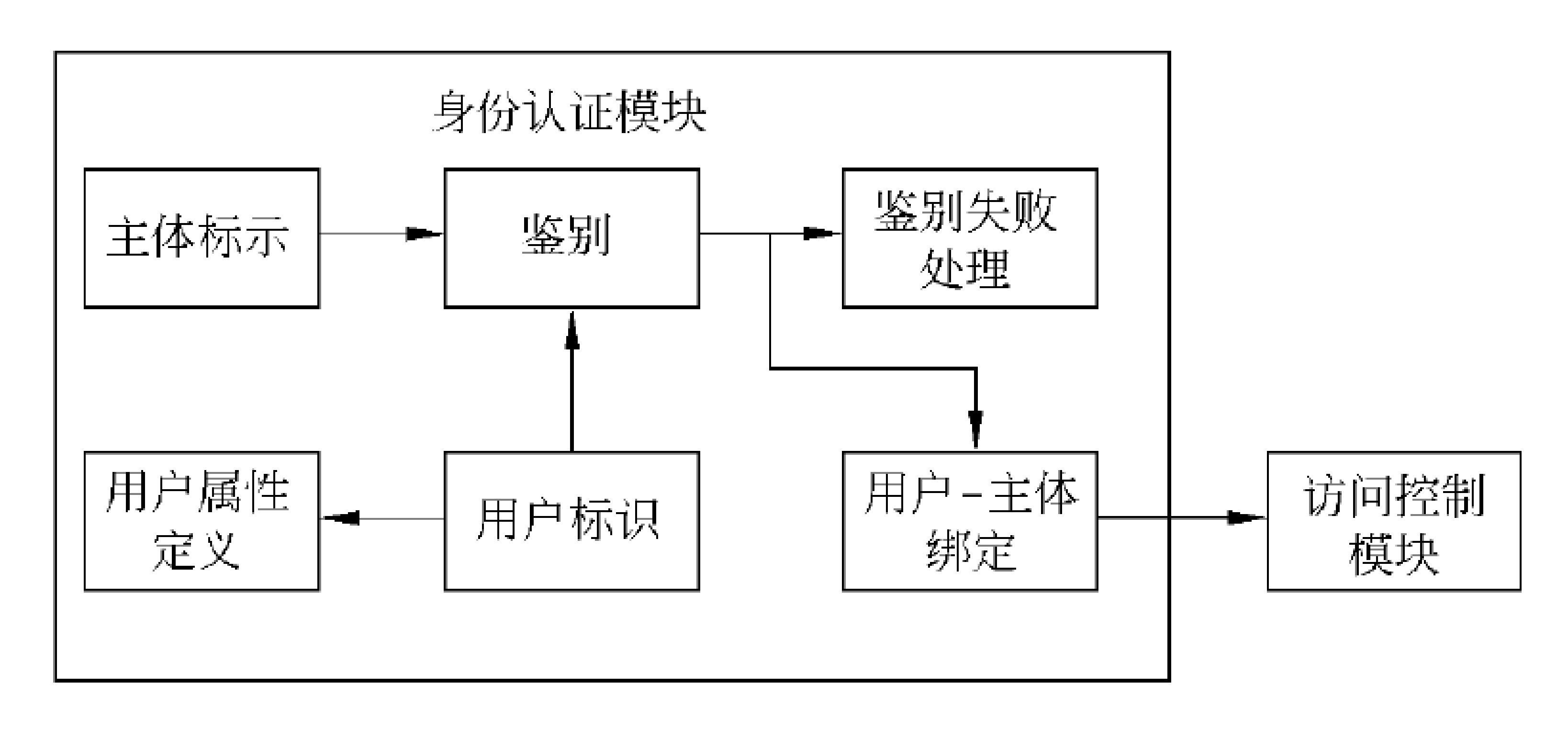



图 2-5 身份认证模块的结构

### 2. 用户属性定义

所有授权用户都有一组用户身份外的安全属性用来执行安全策略。本模块定义用于支持安全策略所需的将用户安全属性与用户相关联的要求。

### 3. 用户-主体绑定

一个已鉴别了的用户，为了使用系统，要先激活一个主体。用户的安全属性（全部或部分地）则与该主体相关联。本模块定义建立和维护用户的安全属性与代表用户活动的主体间关联的要求。

### 4. 鉴别

鉴别机制能满足如下特性：

① 鉴别机制能够检测和防止使用伪造或复制的鉴别数据。

② 支持使用一次性鉴别数据的鉴别机制。

③ 提供和使用不同的鉴别机制，为特定的事件鉴别用户的身份。

④ 重鉴别，要求有能力说明哪些事件用户需要被重新鉴别。

⑤ 在鉴别期间，只提供给用户有限的反馈信息。

本模块可采用的用户鉴别安全机制：采用强化管理的口令鉴别或基于令牌的动态口令鉴别或具有相应安全强度的其他鉴别。

### 5. 鉴别失败处理

为不成功的鉴别尝试次数定义值，以及鉴别尝试失败时的行动。能够在用户鉴别尝试失败了指定的次数后，终止会话建立进程。此外，它还在会话建立进程终止后，直到管理员定义的条件出现前，使用户账号无效，或者使进行尝试的登录点无效（如某工作站）。

## 2.3.2 访问控制模块结构

访问控制模块结构如图 2-6 所示。

### 1. 主体

以标识和鉴别子系统中为主体分配的标识及安全属性为基础。

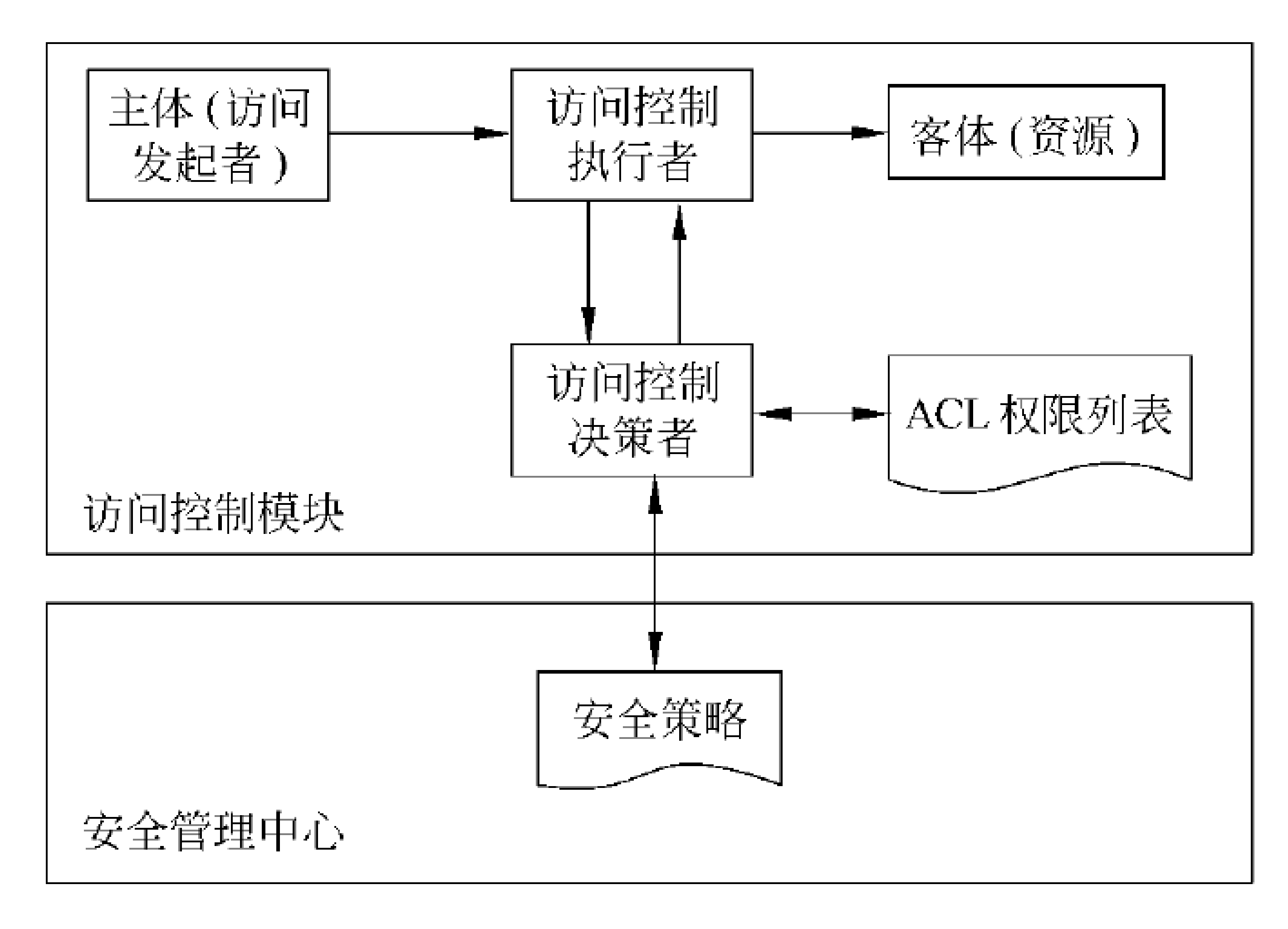



图 2-6 访问控制模块结构图

### 2. 客体

信息的载体。

### 3. 访问控制执行者

执行访问控制机制。在访问控制机制中，由主体代表访问或试图访问客体的人和基于计算机的实体提出访问目标的请求，系统根据决策规则由执行功能对访问请求进行分析、处理，在授权的范围内允许发起者对目标进行有限地访问，确保只有对目标拥有访问权限的主体才能执行。

### 4. 访问控制决策者

表示一组访问控制规则和策略。决策功能控制着主体的访问许可，限制其在何种条件下，为了什么目的，可以访问哪些客体。这些决策以某一访问控制策略的形式反映出来。访问请求通过某个访问控制机制而得到过滤。决策依赖下列信息：主体访问决策信息（绑定到发起者的访问控制信息）；访问请求访问决策信息（绑定到访问请求的访问控制信息）。

### 5. 访问控制表

以文件为中心建立的访问权限表（Access Control Lists，ACLs）。目前，大多数 PC、服务器和主机都使用 ACLs 作为访问控制的实现机制。访问控制表的优点在于实现简单，任何得到授权的主体都可以有一个访问表。

## 2.3.3 数据完整性保护模块结构

数据完整性保护模块结构如图 2-7 所示。

### 1. 运行体拦截

- 运行体拦截模块设置在系统内核中，该模块拦截任何试图执行的对象，并通知文件完整性验证模块对该对象进行验证。

图 2-7　数据完整性保护模块结构

- 运行拦截体的拦截规则可在一定安全范围内由系统管理员通过完整规则管理中心进行设置，以符合用户的完整性需求。

### 2. 对象完整性验证

- 对象完整性验证模块接收运行体拦截模块传送来的试图执行的对象信息。然后按照预定义的流程，根据关键对象校验库中的预存信息以及该对象自身的信息，判断出该对象的完整性状态。然后将该完整性状态交付给安全处理模块。
- 对象完整性验证模块的验证规则可在一定安全范围内通过完整规则管理中心设置，以符合用户的完整性需求。

### 3. 关键对象校验库

- 关键对象校验库模块的主要功能是为对象完整性模块提供验证信息。存储了安全预定义和用户自定义的关键对象的完整性信息。包括关键对象的安全级别、路径、对象内容哈希值、操作、完整性状态几个属性。
- 关键对象校验库模块中的对象一部分是由数据完整性保护子系统预定义的完整性最小集，保证系统核心部分的完整性。
- 关键对象校验库提供了备份与恢复的接口，系统管理员必须定期对对象库进行可信备份。在关键对象校验库被破坏时，对其进行可信恢复。

### 4. 完整性规则管理中心

- 完整性规则管理中心是由系统/安全管理子系统管理，用于维护数据完整性保护模块在安全、有序、合理的状态下进行运行。对关键对象校验库、安全处理模块、运行体拦截模块在授权安全范围内提供设置，以在保证系统最小完整性需求的前提下满足用户对完整性的需求。
- 完整性规则管理中心提供操作界面接口，系统管理员通过完整性规则管理中心对安全处理模块的执行规则和运行体拦截模块的拦截选项进行可选择性配置。

### 5. 安全处理

① 安全处理模块接收对象完整性模块传送过来的对象信息，根据预定义的规则作出

相应的动作，如阻止对象运行、运行对象运行、报警等。

② 安全处理模块的处理动作由数据完整性保护模块预定义。系统管理员也可在其安全授权范围内对处理动作进行个性化定义。

### 6. 审计

① 安全审计对数据完整性保护模块中的关键行为进行详细的审计记录。

② 安全审计对于每一种权限的使用人员的操作都有详细的审计记录。

③ 安全审计将对象完整性验证模块中提供的安全报告进行详细的审计记录。

④ 安全审计提供与审计子系统的接口，按审计子系统的需求提供审计数据。

## 2.3.4 客体安全重用模块结构

客体重用模块结构如图 2-8 所示。

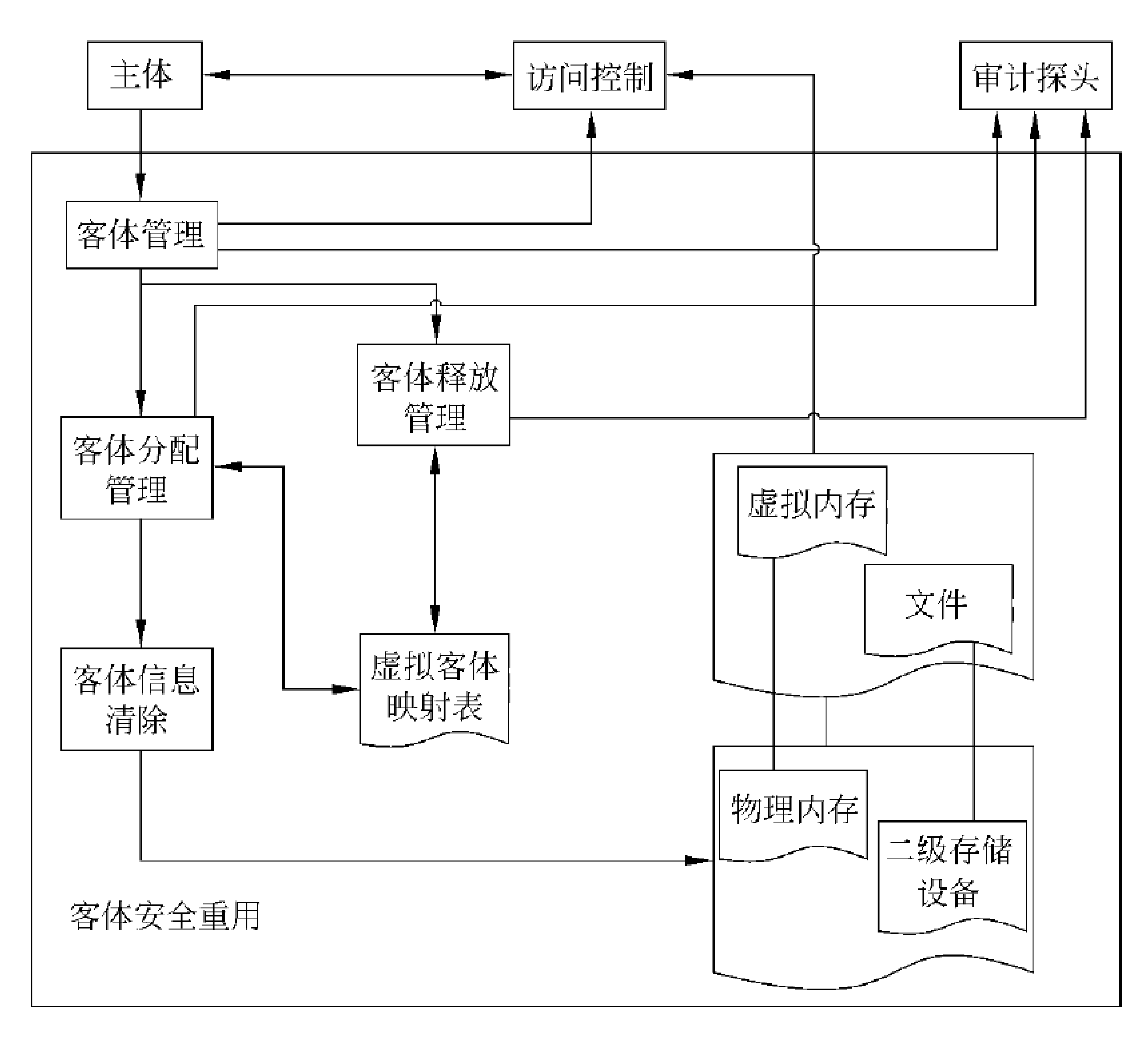



图 2-8 客体重用模块结构

### 1. 客体管理

主体申请使用新的客体或释放旧的客体时，客体管理拦截到该申请。客体管理提供给主体分配和释放客体的接口，解析主体的动作，并决定对客体的操作。

### 2. 客体分配管理

根据需求，将所请求的客体分配给主体。在客体分配前必须调用客体信息清除模块对客体中残存的信息进行彻底清除。

### 3. 客体释放管理

当客体需要被重用时，或客体不再被主体需要时，客体释放管理将此客体放入可用的客体池中。

### 4. 客体信息清除

对释放的客体进行信息清除。最简单的方法是在客体的存储空间内填充全 0、全 1 。对于更高安全级别，可以采取多种填充方式反复进行，以完成对客体物理介质进行不可恢复性消磁。

### 5. 审计探头

客体重用模块中的关键操作信息都按安全需求进行安全审计。该审计探头提供与审计子系统的接口，按审计模块的需求提供审计数据。

### 6. 虚拟客体映射表

此实体为数据表，提供主体可见的虚拟客体到实际物理客体如内存和二级存储设备的映射。

## 2.4 安全区域边界子系统的设计和实现

区域边界子系统总体结构如图 2-9 所示。

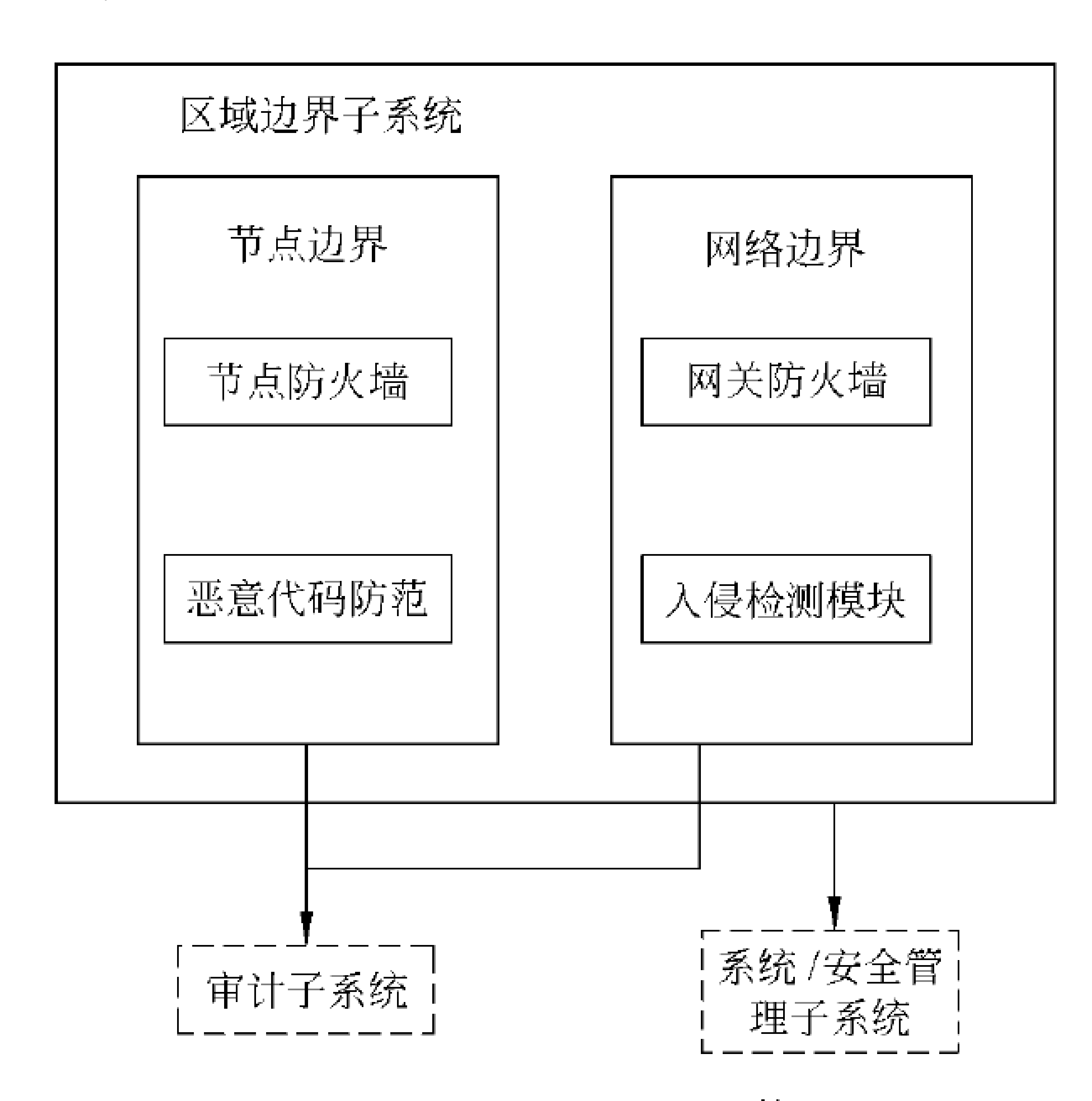



图 2-9　区域边界子系统总体结构

① 防火墙模块：防火墙进行信息过滤，来保护计算机网络免受非授权人员的骚扰与黑客的入侵。

② 入侵检测模块：监视受保护系统的状态和活动，采用异常检测或误用检测的方式，发现非授权的或恶意的系统及网络行为，为防范入侵行为提供有效手段。

③ 恶意代码防范模块：基于病毒定义码匹配规则、异常行为分析(神经网络等算法和技术)技术的分析与实现。

## 2.4.1 防火墙子模块结构

防火墙子模块的结构如图 2-10 所示。

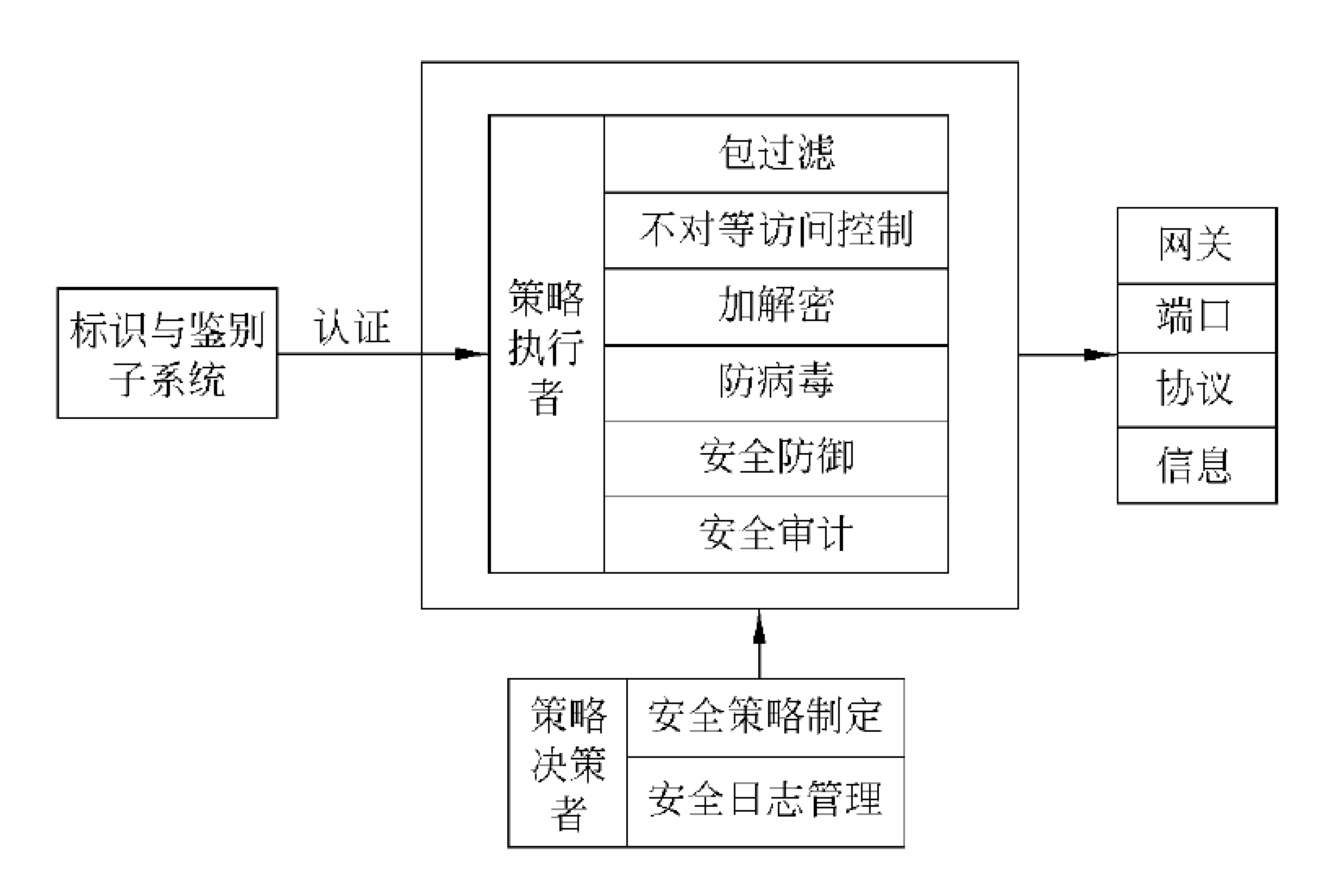



图 2-10 防火墙子模块的结构

### 1. 加解密支持

支持 VPN 加密标准，例如国内专用的加密算法。除了 VPN，加密除了在保护传输数据以外，还应用于其他领域，如身份认证、报文完整性认证，密钥分配等。提供基于硬件的加密，以提供更快和更高的加密强度。

### 2. 管理员认证支持

认证类型灵活，防火墙支持的身份认证协议，一般情况下具有一个或多个认证方案，如 RADIUS、Kerberos、TACACS/TACACS+、口令方式、数字证书等，使防火墙能够为本地或远程用户提供经过认证与授权的网络资源的访问，且防火墙管理员必须决定客户以何种方式通过认证。

### 3. IP 访问控制和不对等访问控制

通过防火墙的包内容的过滤，对明确定义的数据包(如 RFC 中定义的)要定义过滤规则集，由若干条规则组成，涵盖对所有出入防火墙的数据包的处理方法；对于没有明确定义的数据包，应该有一个默认的处理方法；过滤规则应易于理解和易于编辑修改；同时应具备一致性检测机制，防止冲突。其中 IP 包过滤的依据主要是根据 IP 包头信息，如源地址和目的地址进行过滤。

在应用层提供代理支持：防火墙支持应用层代理，包括 HTTP、FTP、TELNET、SNMP 等。代理服务在确认客户端连接请求有效后接管连接，代其向服务器发出连接请求，代理服务器根据服务器的应答，决定如何响应客户端请求。

### 4. 安全防御功能

支持病毒扫描：包括扫描电子邮件附件中的 DOC 和 ZIP 文件，FTP 中的下载或上载文件内容，以发现其中包含的危险信息。

提供内容过滤：防火墙能在 HTTP、FTP、SMTP 等协议层，根据过滤条件，对信息流进行控制，防火墙可以允许通过、修改后允许通过、禁止通过、记录日志、报警等。过滤内容要包括 URL、HTTP 携带的信息，如 Java Applet、JavaScript、ActiveX 和电子邮件中的 Subject、To、From 域等。

能防御 DOS 攻击：防火墙通过控制、检测与报警等机制，在一定程度上防止或减轻 DOS 黑客攻击。

### 5. 管理功能

需管理的管理员的行为主要包括：通过防火墙的身份鉴别，编写防火墙的安全规则，配置防火墙的安全参数，查看防火墙的日志等。防火墙本身的管理一般有本地管理和远程管理。

① 本地管理：管理员通过防火墙的 Console 口进行配置管理。

② 远程管理：管理员通过 FTP、TELNET、HTTP 进行配置管理。

### 6. 安全审计

规定了对于符合条件的报文作日志，并提供日志信息管理和存储方法；提供自动日志扫描具有日志的自动分析和扫描功能，提供自动报表、日志报告书写器；提供告警机制，在检测到入侵网络以及设备运转异常情况时，通过告警来通知管理员采取必要的措施，包括 E-mail、呼机、手机等。提供简要报表(按照用户 ID 或 IP 地址)，并能分类打印；提供实时统计即在日志分析后所获得的智能统计结果，一般是图表显示。

## 2.4.2　入侵检测子模块结构

入侵检测系统分为四个基本模块：事件产生器、事件分析器、响应单元和事件数据库，其中的事件是 IDS 需要分析的数据。这四个模块只是逻辑实体，一个模块可能是某台计算机上的一个进程甚至线程，也可能是多个计算机上的多个进程，这些模块以 GIDO (统一入侵检测对象)格式进行数据交换。入侵检测子模块的结构如图 2-11 所示。

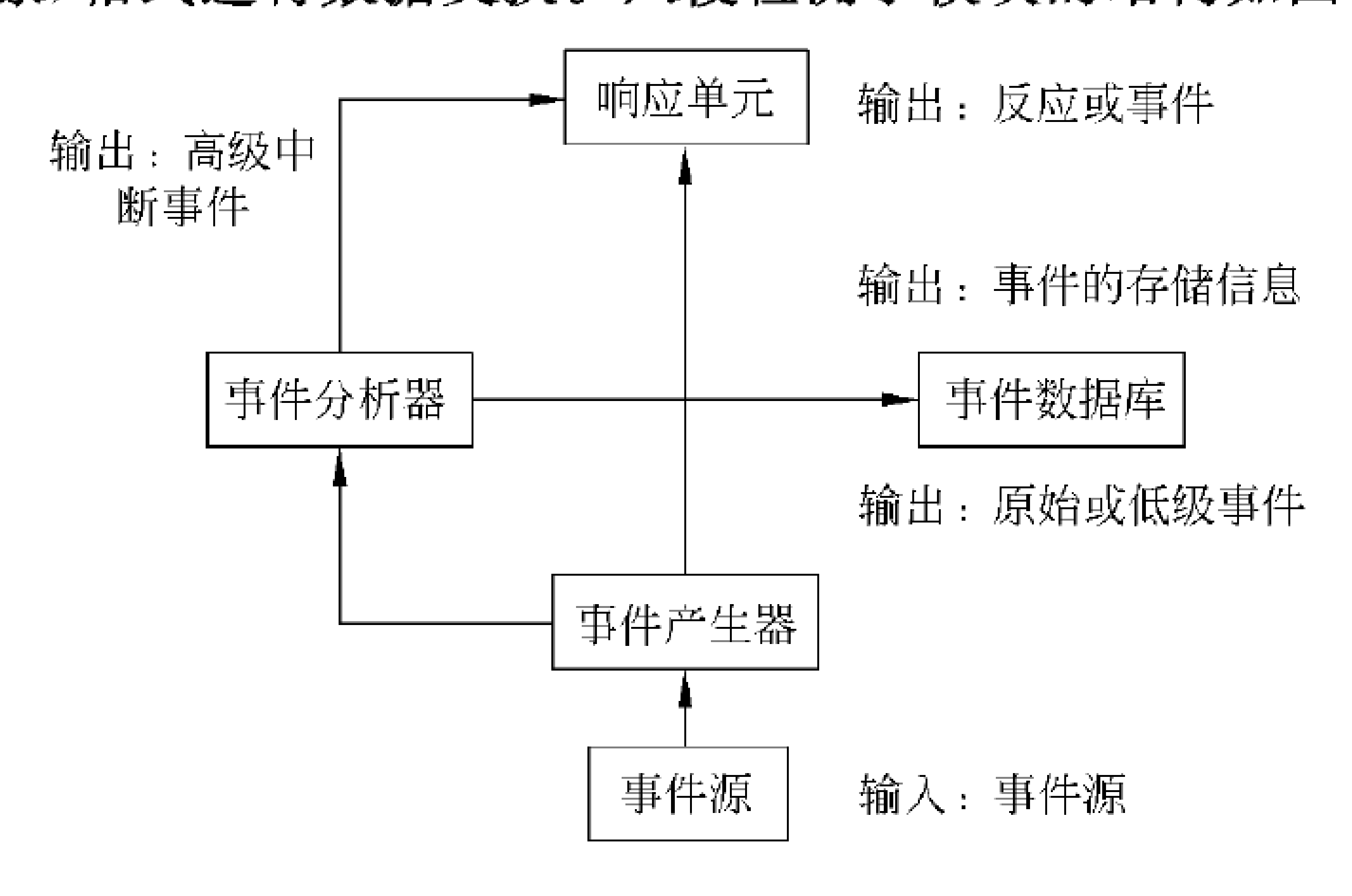



图 2-11　入侵检测子模块的结构

### 1. 事件产生器

事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

### 2. 事件分析器

事件分析器分析得到数据，并产生分析结果。对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。入侵检测分为两类：一种基于标志(signature-based)，另一种基于异常情况(anomaly-based)。

### 3. 响应单元

响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。

### 4. 事件数据库

事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

## 2.4.3 恶意代码防范模块结构

其提供一套完善的恶意代码防范体系，在恶意代码传播的途径上拦截数据，分析判断出数据中是否存在恶意行为。恶意代码防范子模块的模块关系如图 2-12 所示。

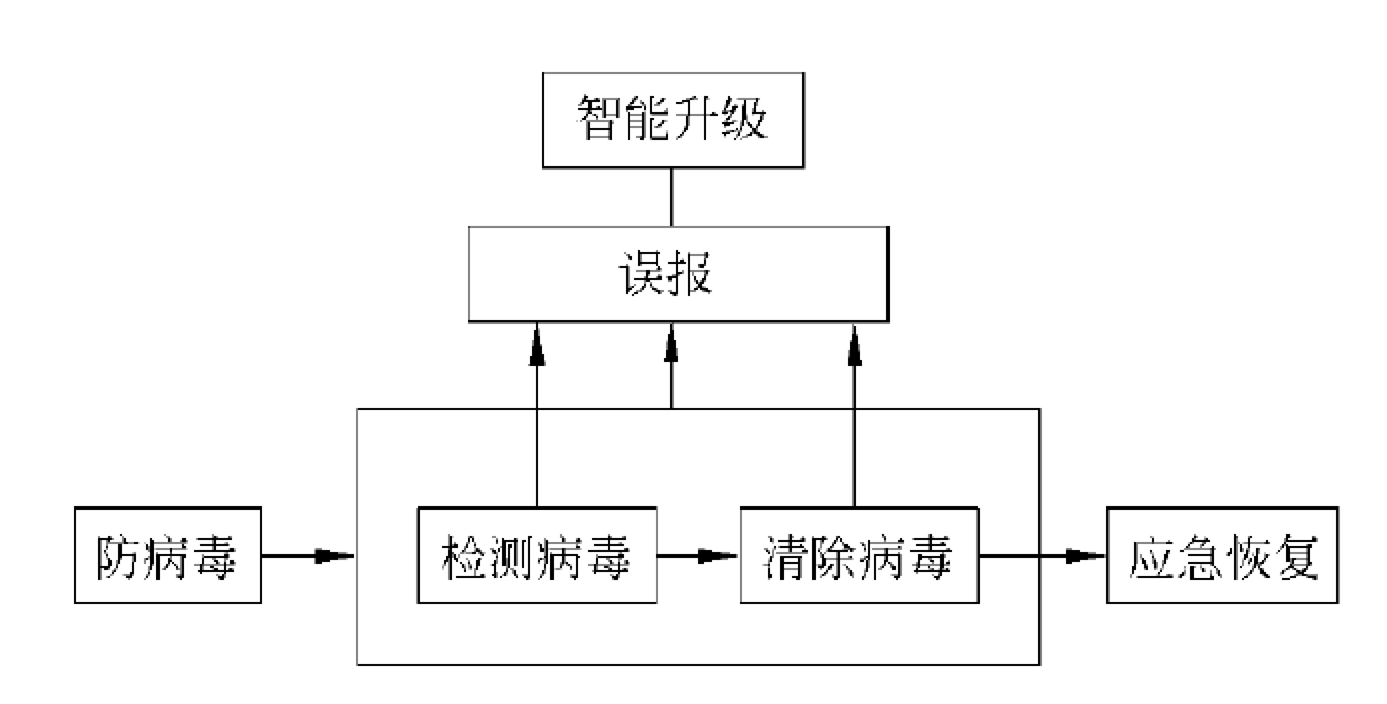



图 2-12　恶意代码防范子模块的模块关系

### 1. 防病毒

① 病毒样本库中的病毒样本从以下途径进入计算机系统时发出警报：

存储介质、网络、电子邮件；

② 设定满足病毒传染、发作的条件，然后激活病毒，病毒防治产品能够阻止病毒的传播、破坏；

③ 对病毒入侵情况记录到报告文件；

④ 网络产品发现病毒时通知网络管理员或用户。

### 2. 检测病毒

① 对病毒样本基本库至少能检测其中的 95%；

② 对流行病毒样本库至少能检测其中的 98%；

③ 对特殊格式病毒样本库至少能检测其中的 95%。

### 3. 清除病毒

① 清除病毒时，具有备份感染宿主的功能；

② 对病毒样本基本库至少能清除其中的 90%；

③ 对流行病毒样本库至少能清除其中的 95%。

### 4. 误报

对检验机构指定文件组成的误报检验样本库的误报率不能高于 0.1%。

### 5. 应急恢复

正确备份、恢复主引导记录，正确备份、恢复引导扇区。

### 6. 版本智能升级

病毒防治产品在通过互联网或者存储介质进行版本升级时，只需要下载或拷贝升级文件的修改或增加部分，以提高用户升级的效率。

## 2.5 安全通信网络子系统的设计和实现

二级通信网络子系统负责保证安全系统在通过网络进行跨域访问时的安全，同时阻止外部网络通过交换机非法访问内部安全系统。对网络安全审计、网络恶意代码防杀、网络备份/冗余与故障恢复、网络应急处理和网络及网络设备进行管理。通信网络子系统的组成如图 2-13 所示。

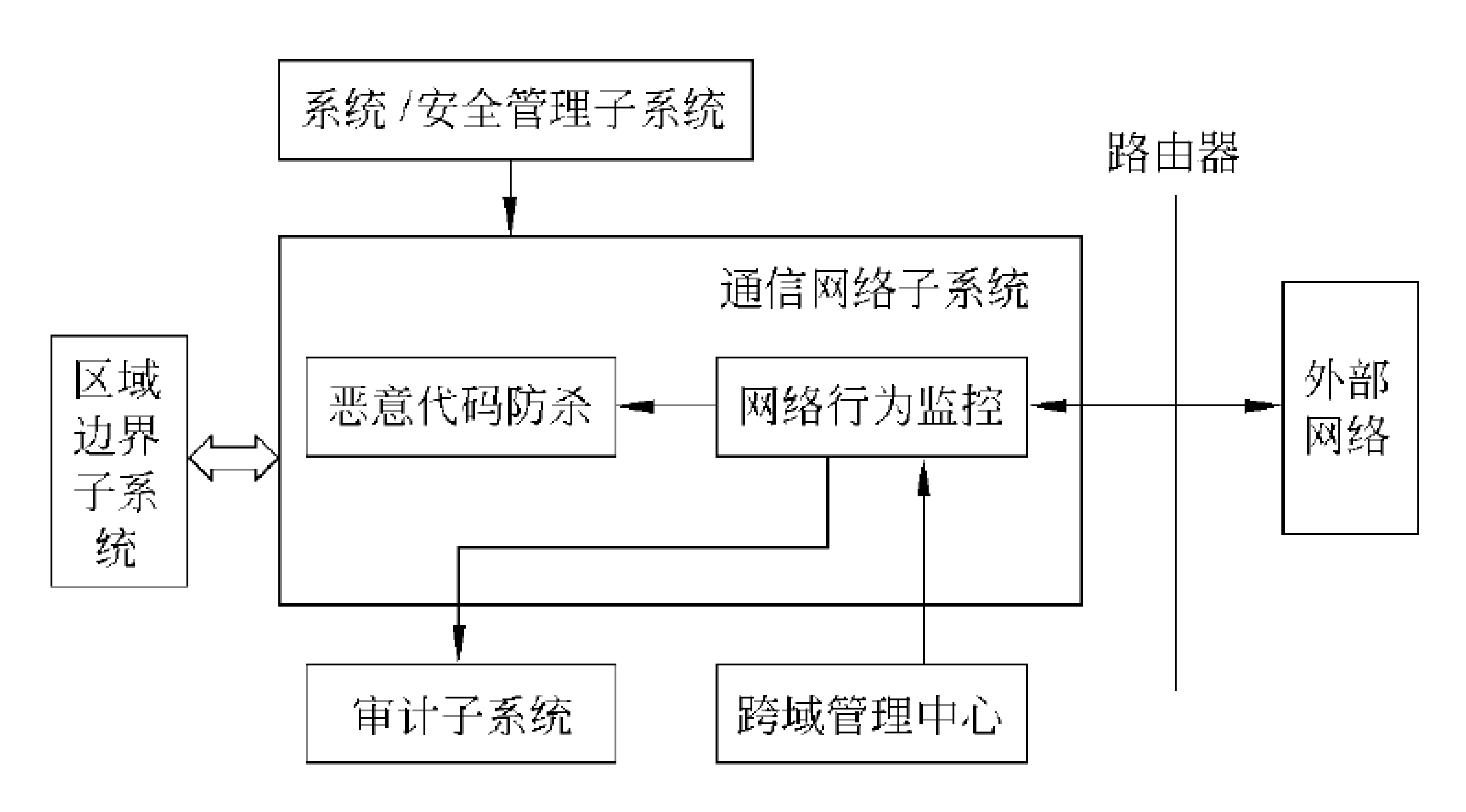



图 2-13 通信网络子系统的组成

① 网络行为监控负责对外网进行监控，按照策略进行过滤，对恶意的网络攻击拦截，递交审计子系统审计或递交给恶意代码防杀模块处理。

② 恶意代码防杀具有识别网络恶意代码能力、清杀恶意代码能力、清杀恶意代码失败后的防护能力、定期扫描及分层分级管理能力和智能升级能力。

## 2.6 安全管理子系统的设计和实现

系统/安全管理子系统主要由管理控制台、审计模块、策略库和几个与安全相关的服务器组成。系统/安全管理子系统的组成结构如图 2-14 所示。

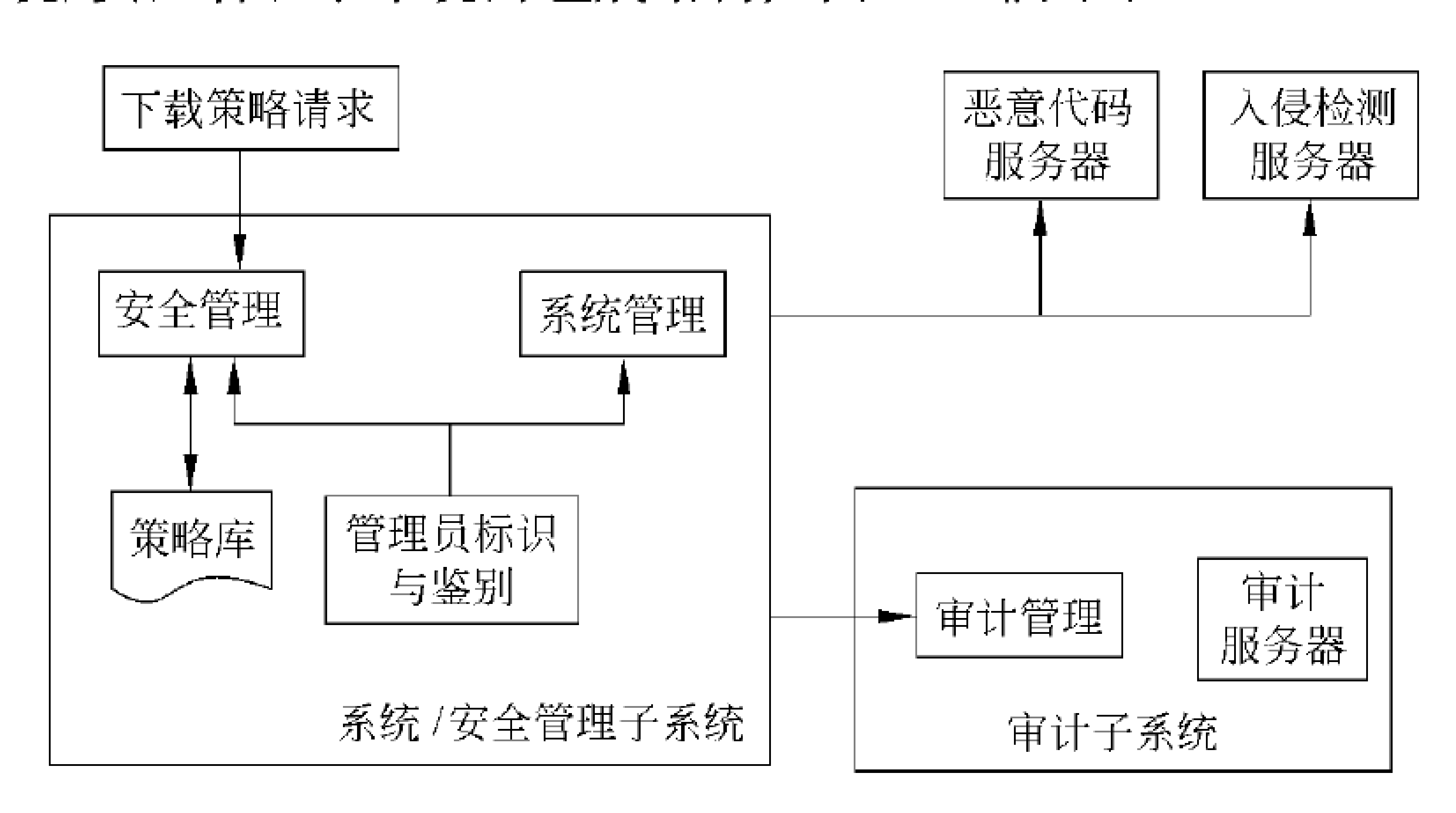



图 2-14 系统/安全管理子系统的组成结构

### 1. 管理控制台

管理员通过控制台对整个系统的安全策略进行配置与控制。从该控制台登录并管理系统的有下面三类管理员。

(1) 系统管理员

主要负责主机系统的运维、监督和管理工作，定期编写主机系统运维与应用性能分析报告，及时发现系统问题，对系统故障及时作出应急处理。

(2) 安全管理员

负责整个系统的安全管理工作，定期编写安全威胁分析报告，对安全事件及时作出反应。并负责网络运维的管理工作，定期编写网络运维与性能分析报告，对网络故障及时作出应急处理。

(3) 审计管理员

对各种应用及安全事件进行审计、分析和报告，对历史数据进行备份。

### 2. 安全管理模块

主要负责主机系统的运维、监督和管理工作。

### 3. 系统管理模块

负责整个系统的安全管理工作和网络运维的管理工作。

### 4. 策略库

放置各类安全策略，当计算环境子系统，区域边界子系统，通信网络子系统需要下载安全策略时，便需要向安全管理中心提出请求，从策略库中下载相应策略。

### 5. 恶意代码服务器，入侵检测服务器

存放恶意代码模块和入侵检测模块所需安全数据，并且存放这些模块产生的安全数据，例如入侵检测系统中的漏洞知识库。

## 2.7　审计子系统的设计和实现

审计子系统模块结构如图 2-15 所示。

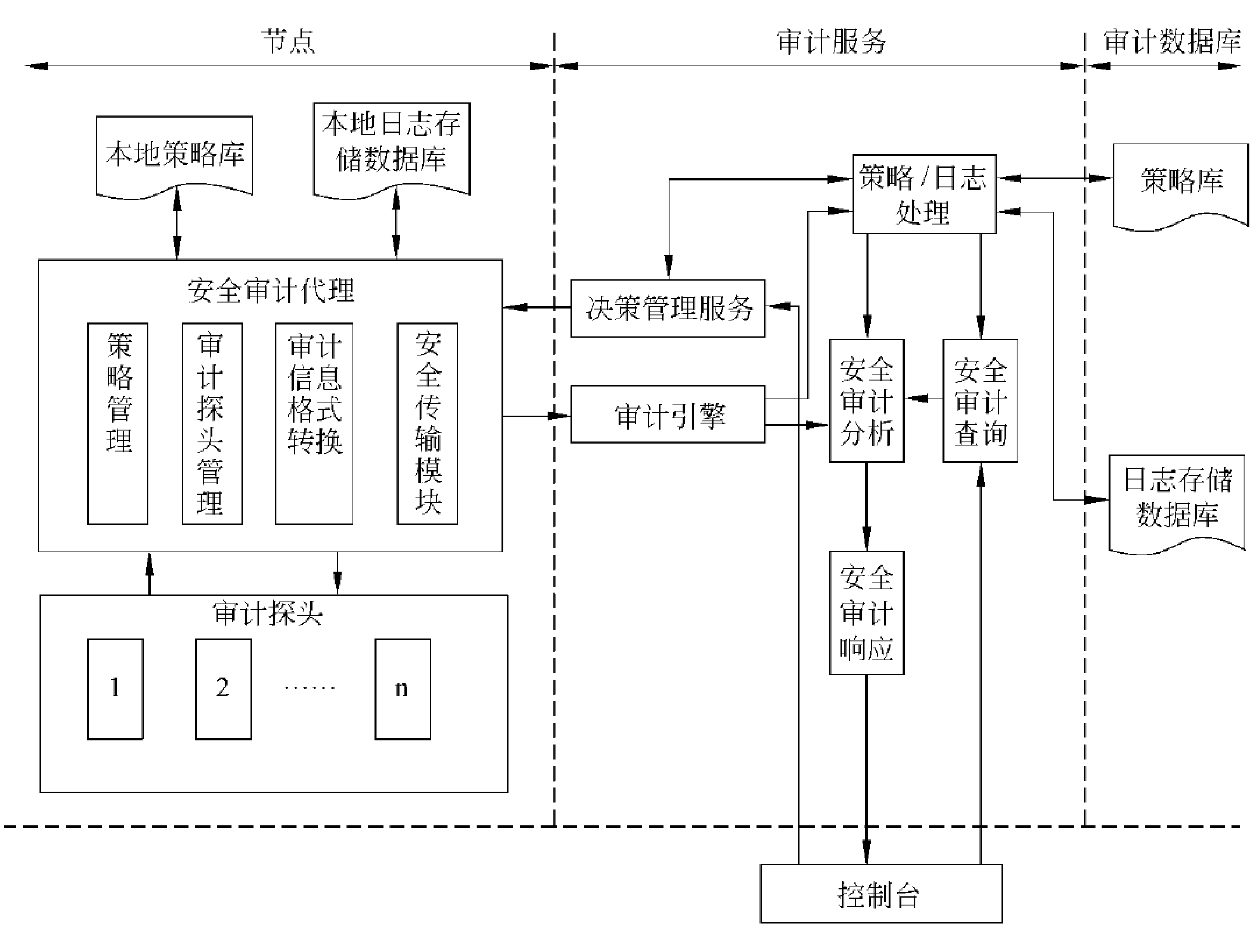



图 2-15　审计子系统模块结构

### 1. 审计探头

获取监控范围内的审计信息。

### 2. 安全审计代理

协调调用审计探头管理模块、策略管理模块、审计信息格式转换模块、安全传输模块，实施审计信息收集、转换、传输和策略模板下发功能。

安全审计代理模块调用审计探头管理注册、删除审计探头；调用策略管理模板对下载的策略形成策略模板，下发给特定匹配的审计探头；从审计探头获取审计信息后，调用审计信息格式转化模块进行标准格式转换；调用安全传输模块将标准格式日志信息加密，传输至审计服务器进行审计分析。安全审计代理模块调用关系如图 2-16 所示。

① 安全审计代理调用审计探头管理模块注册/删除审计探头。

② 安全审计代理从服务器端策略库获得策略后，调用策略管理模块形成策略模板，

下发给相匹配的审计探头。

③ 各种审计探头获取审计信息发送给安全审计代理后，安全审计代理调用审计信息格式转换模块形成统一的日志格式信息，作为本地日志存储和安全审计分析的数据源。

④ 安全审计代理获得统一日志格式信息，调用安全传输模块加密后，再传输至安全审计分析。

⑤ 审计探头管理模块调用审计探头模块，注册或删除审计探头。

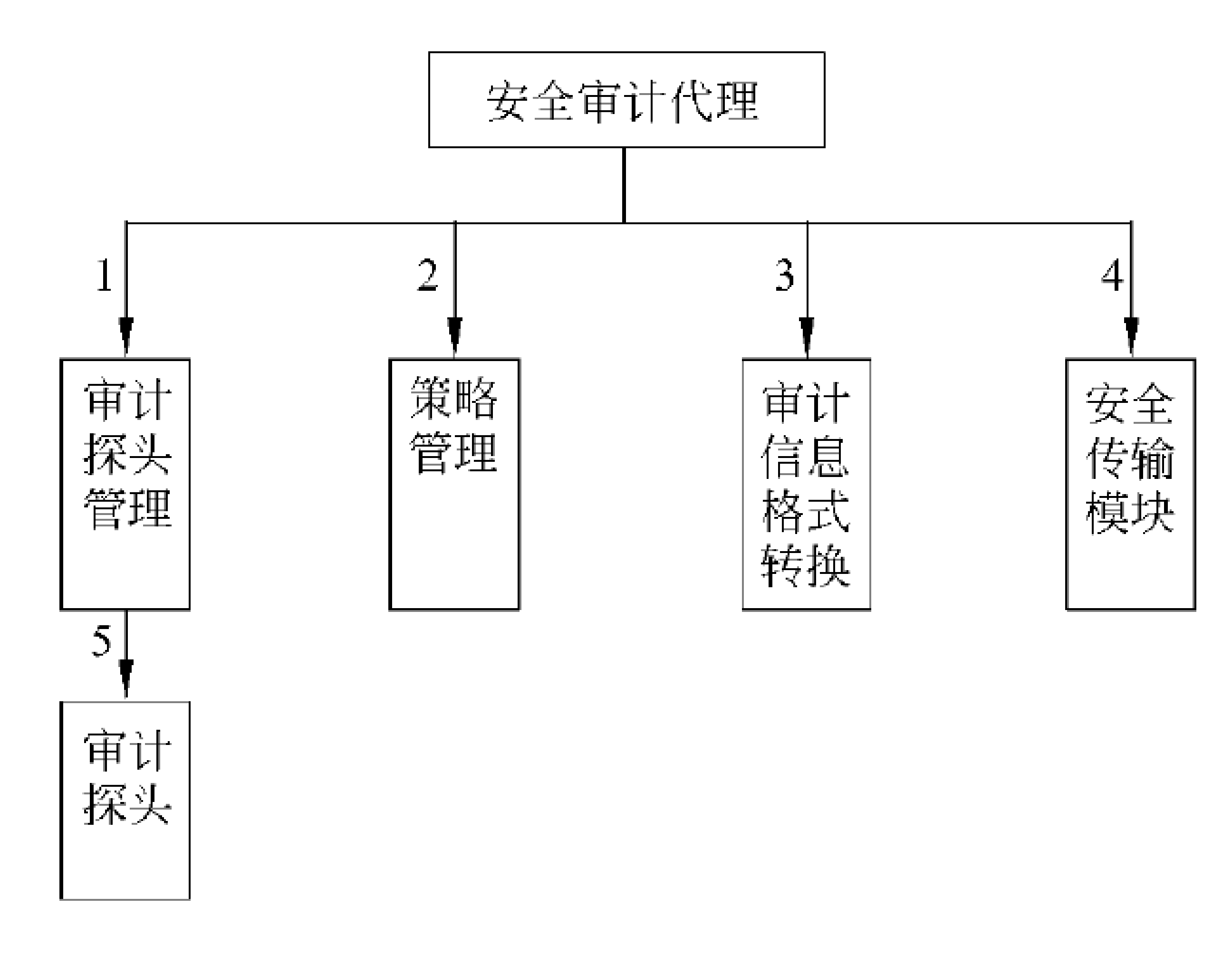



图 2-16 安全审计代理模块调用关系

### 3. 日志存储数据库

分为本地日志存储数据库和服务器端日志存储数据库。本地日志存储数据库是在节点备份审计探头采集的本地审计日志，以防止网络不通的情况下，审计信息的丢失；服务器端日志存储数据库是存储这个信息系统获取的供审计分析的日志信息。

### 4. 审计引擎

开启和关闭审计引擎，通信审计代理进行审计信息加密/解密传输，交由安全审计分析模块对信息进行审计分析。

### 5. 策略管理服务

开启策略管理下载服务，形成三重结构，防止直接读取策略库，而对策略库构成安全威胁，保证了策略数据的安全性。提交策略下载请求给策略/日志处理模块，获取策略库中的策略。

策略管理服务在获取策略/日志处理模块准备发送策略的就绪状态时，提示安全审计代理调用策略管理模块处理策略，形成策略模板。

### 6. 安全审计分析

对信息系统审计日志记录进行安全性分析，对用户行为进行监控，防止用户越权使用，检测系统资源使用状况，保证系统的安全性。这种分析可用入侵检测来支持，或对即将来临的安全侵害作出自动响应。

#### 7. 策略/日志处理

本模块提供一种策略下载/存储请求与策略库/日志存储库之间的安全通道，防止直接对策略库和日志存储库的读取，从而保证了策略库和日志存储库的数据不被破坏。

#### 8. 安全审计响应

同时监控审计探头管理模块和审计服务器端的安全威胁响应，可分为短消息提示、报警等不同级别的响应方式。

#### 9. 安全审计查询

为第三方查询提供了接口，方便审计管理员在控制台查询有关的审计信息。

#### 10. 策略库

分为本地策略库和服务器端策略库，本地策略库是策略管理模块请求下载策略在本地的存储备份；服务器端策略库是存储整个信息系统中审计管理员、系统管理员、安全管理员（二级中系统管理员和安全管理员可同为一组）制定的安全策略。

#### 11. 安全传输模块

安全传输模块将审计代理调用审计信息格式转换模块产生的统一格式信息进行安全性加密，以保证信息的完整性和保密性，再传输到审计服务器端；在审计服务器端，安全传输模块将统一格式审计信息进行解密后，递交给安全审计分析模块分析并存储。

#### 12. 策略管理

从审计服务器端的策略库下载策略到本地，并将从策略库下载的策略按不同类型的审计探头形成相应的策略模板，提供给审计探头管理模块。策略管理模块还提供可扩展的策略模板接口，可以定制新的策略模板类型，为三级、四级安全系统提供接口。

#### 13. 审计探头管理

注册新的与策略模板匹配的审计探头；删除审计探头。

#### 14. 审计信息格式转换

将审计信息转换成审计子系统定义的标准格式。

此模块同样提供可扩展的格式标准接口。

## 2.8 典型应用子系统的设计和实现

根据二级安全应用平台安全保护的要求，应用系统自身要提供身份认证、访问控制和应用行为审计等基本功能，并实现用户使用公文流转系统过程中鉴别信息存储与传输的保密性与完整性，对软件容错也有相应要求。在二级安全应用平台应用演示环境中具体安全措施如图 2-17 所示。

#### 1. 计算环境子系统

① 在使用公文流转系统的服务器和终端上安装网络通信防病毒系统（具有桌面防火

墙功能)的客户端时,接受网络通信防病毒的统一管理,防范、阻止病毒、蠕虫、木马和间谍软件等恶意代码的传播。

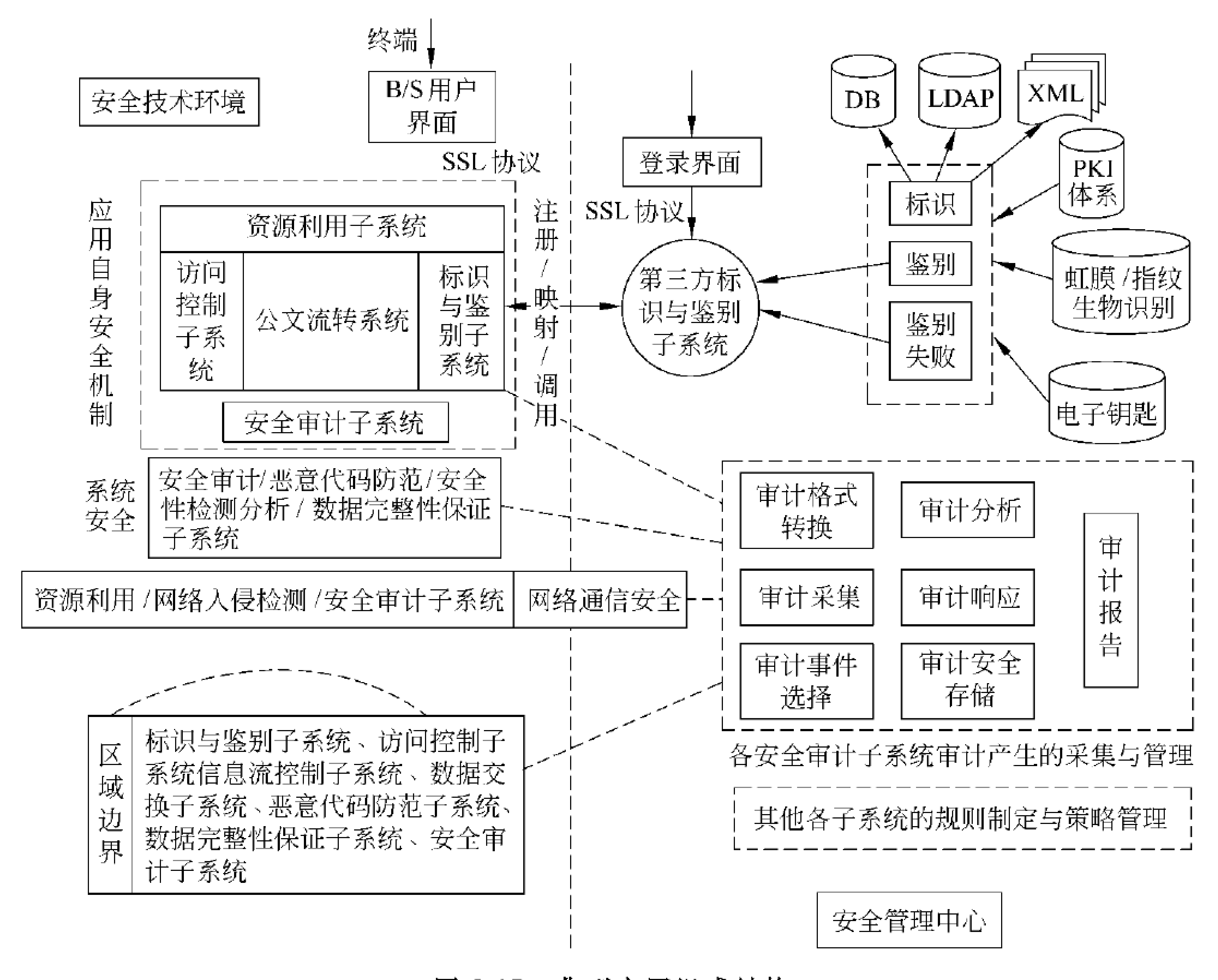



图 2-17 典型应用组成结构

② 配置操作系统的安全策略,并利用操作系统的备份机制,定期进行系统与数据备份,应对出现的人为或自然造成的破坏事件。

③ 结合终端操作系统用户认证机制进行身份认证,防止用户欺骗和假冒。

④ 在公文流转系统服务器上安装审计代理。

⑤ 应用自身的安全:

- 支持采用数字证书、智能电子钥匙等第三方身份鉴别方式实现身份认证,登录失败结束会话;
- 公文流转系统管理员设定访问控制策略,依据策略控制用户对模块的使用;
- 公文流转系统审计管理员对应用系统的每个用户行为进行安全审计;
- 公文流转系统支持 SSL 协议保证通信保密性和完整性;公文流转系统限制应用系统的最大并发会话连接数;
- 公文流转系统限制单个账户的多重并发会话。

⑥ 公文流转系统数据库中数据定期定时备份。

### 2. 通信网络子系统

(1) 网络通信管理系统

为了保证公文流转系统的高可用性,需要网络通信管理系统实时监控网络通信拓扑、

网络通信和主机服务器的运行状态，发现异常及时报警。

(2) 网络通信安全审计

对用户访问公文流转系统的所有行为进行监控与审计，并可以基于协议还原查看用户对公文流转系统进行的所有操作。

### 3. 区域边界子系统

对用户通过网络通信访问公文流转系统的行为进行审计。

① 使用防火墙控制用户能访问公文流转系统的协议和端口，其他的协议和端口全部关闭，降低病毒、蠕虫、木马和间谍软件等恶意代码传播的机会；

② 在防火墙上选配防病毒引擎，禁止病毒、蠕虫、木马和间谍软件等恶意代码通过区域边界传入计算环境。

### 4. 安全管理中心子系统

① 对公文流转系统服务器的性能指标和运行状态等进行监控和管理，发现问题及时通知管理员；

② 公文流转系统服务器端和客户端恶意代码防护的查杀、定期扫描、及时升级等管理；

③ 对用户访问公文流转系统的网络通信行为，用户在终端上的所有行为(包括操作公文流转系统客户端的行为)，用户在应用系统中的行为进行审计、关联分析和综合管理。

# 2.9 示范环境功能使用操作演示

## 2.9.1 自主访问控制系统

对终端系统的访问资源进行控制，所提供的控制是可以配置的，并以中心进行管理。对终端用户的可执行程序授权，对用户访问系统资源及网络服务加以控制，并及时记录用户的行为事件产生审计信息。对终端系统进程实施访问控制，并产生审计信息。

自主访问控制系统分为管理控制台和客户端，具体介绍如下所述。

### 1. 安全管理中心

安全管理中心登录界面如图 2-18 所示。

依据三员分离的原则，在管理中心中存在三类操作人员。

(1) 系统管理员

系统管理员主要是对系统的资源和运行进行配置、控制和管理，包括：用户身份管理，系统资源配置，系统加载和启动。

(2) 安全管理员

安全管理员主要是对主体、客体进行统一标记，对主体进行授权，配置统一的安全策略。

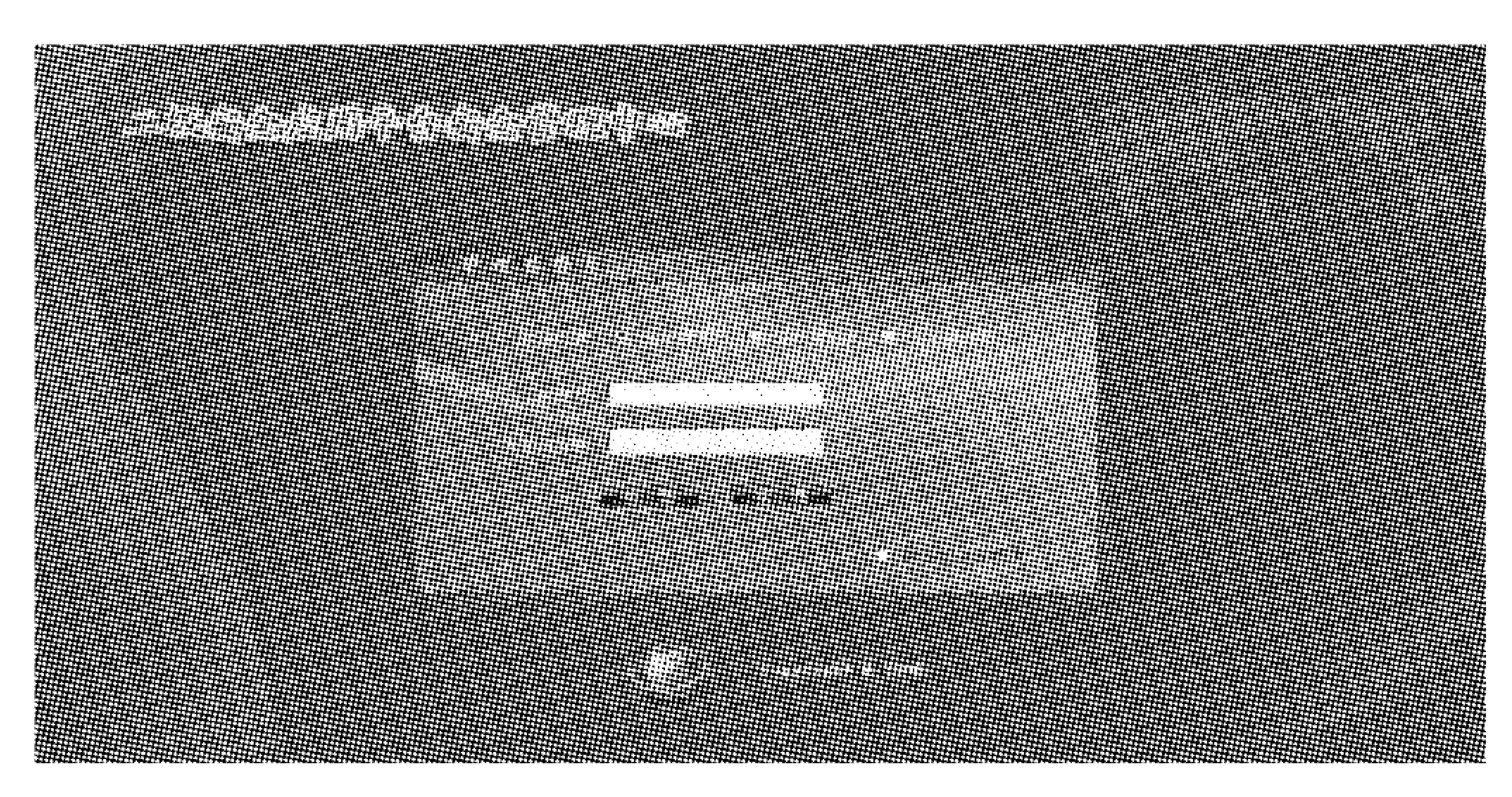


图 2-18 安全管理中心登录界面

(3) 审计管理员

审计管理员主要是按安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储管理和查询。

### 2. Windows 二级安全操作系统

安装 Windows 二级操作系统，并由安全管理中心统一管理，在用户登录 Windows 系统时需使用已授权的硬件令牌(USB-KEY)登录，实施双因子身份认证，具有更高的身份鉴别功能，如系统资源访问受到控制，拒绝信息的非法访问，恶意代码防范，拒绝恶意木马，病毒对系统造成的危害。

### 3. Linux 二级安全操作系统

安装 Linux 二级安全操作系统，并由安全管理中心统一管理，在用户登录 Linux 系统时需使用已授权的硬件令牌(USB-KEY)登录，实施双因子身份认证，具有更高的身份鉴别功能，系统资源访问受到控制，拒绝信息的非法访问。

## 2.9.2 综合审计管理系统

综合审计管理系统主要是对交换机、防火墙、Windows 终端、Linux 终端、网关等各个设备的审计信息通过审计探头采集，并上传到综合审计管理系统，由审计系统进行统一管理、分析、分类查询、存储。

综合审计管理系统分为管理控制台服务器端和客户端(审计探头)，具体介绍如下所述。

### 1. 管理控制台

管理控制台界面如图 2-19 所示。

管理业务主要包括节点信息维护管理、探头类型维护管理、策略维护管理、审计记录查询。

① 节点维护：节点 ID 是分配给客户端探头的唯一 ID 号，探头在初始配置时需要输

图 2-19　管理控制台界面

入此 ID 号，并由审计服务端进行验证。具体操作有添加、修改、删除节点。

② 探头类型维护：探头类型分 Windows 探头、Linux 探头、交换机探头、防火墙探头、客体安全重用探头、网关探头。对不同设备及系统部署不同的探头类型。

③ 策略维护：策略维护主要是配置探头按时间去采集审计信息，对探头的开启/关闭进行配置。

④ 审计记录查询：主要是按时间、节点 ID、探头类型检索审计信息。

### 2. 审计探头

客户端程序(审计探头)，根据综合管理系统配置的策略去采集设备上的审计信息，并上传到审计服务器。

## 2.9.3　剩余信息保护系统

剩余信息保护系统主要是对客体资源进行监控和管理，在该客体资源重新分配前对其原使用者的信息进行清除，以确保系统的重要信息不被泄露。

剩余信息保护运行为 DOS 窗口，如图 2-20 所示，具体介绍如下所述。

① 手动启动及时生效，运行 ord. uil. exe 剩余信息保护程序，在 DOS 命令行输入 start demand 来启动程序。

② 自动启动，运行 ord. uil. exe 剩余信息保护程序，在 DOS 命令行输入 start auto 来启动，及时生效并在每次系统启动时自动启动剩余信息保护程序。

③ 关闭剩余信息保护程序，正常启动后，在 DOS 命令行输入 stop ord 来关闭。

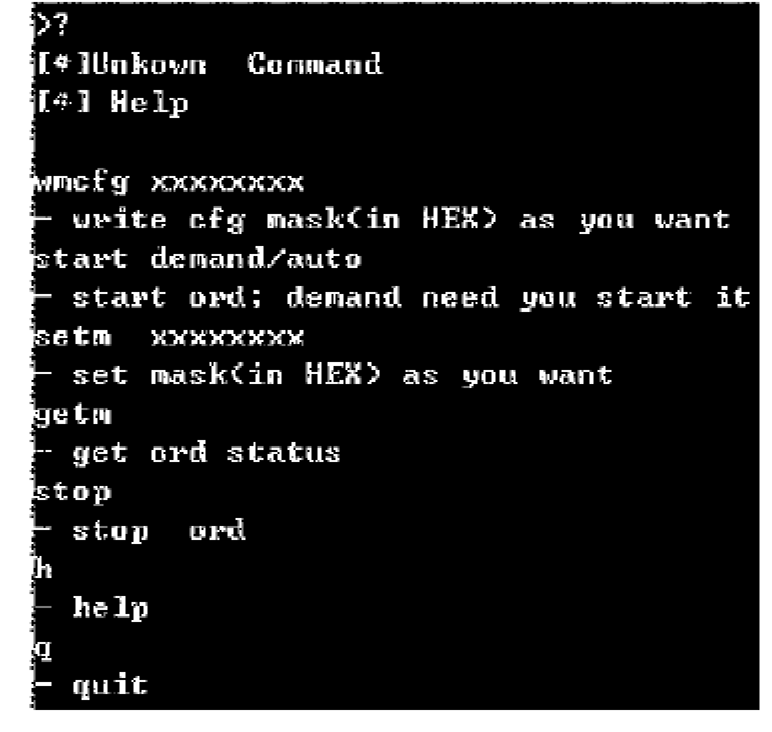



图 2-20　剩余信息保护运行窗口

# 第3章 三级信息系统安全设计和实现

## 3.1 安全功能和总体结构

三级安全应用平台以 GB 17859—1999 等国家标准为基础，依据国家标准对三级安全应用平台的安全要求，以信息标记为手段，以强制访问控制技术为核心，以安全易用为目标，采用系统集成创新的方法，构建三级安全应用平台。防止信息泄露、身份假冒、非授权访问、中间人攻击等，解决三级安全应用平台的安全问题。

三级安全应用平台基本结构如图 3-1 所示。

三级安全应用平台由业务部门计算环境、数据中心计算环境、移动终端和安全管理中心组成。

数据中心计算环境部署典型应用的服务器和数据库，是三级安全应用平台的应用服务提供者和数据集中存放地。业务部门计算环境模拟典型应用中各种类型的访问终端，同时在业务部门计算环境中部署了面向部门开放的内部服务器，供部门内部人员使用。移动终端模拟通过网络接入数据中心计算机环境的移动用户。安全管理中心负责整个三级安全应用平台的主体安全标记、客体安全标记、网络强制访问控制、系统强制访问控制等进行安全管理，部署了三级 VPN 管理系统、三级授权管理系统、三级认证系统、三级安全审计系统等服务器。

从第三级开始对安全功能的设置和安全强度的要求等方面均有明显提高。增加了标记和强制访问控制功能。对所有主体及其所控制的客体(例如，进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。

三级安全应用平台强制访问控制系统流程如图 3-2 所示。

执行主体(应用、代表用户、代表系统)提出访问请求，策略审查模块对主体提出的请求与访问控制列表对比，匹配则允许，不匹配则执行等级改变。但是为了检查该访问请求是否符合系统安全策略，访问控制模块需要与标识管理模块通信，以获得访问请求中主客体的安全标识。在此基础上，强制访问控制模块依据系统符合性检查策略判断该请求是否安全，如果检查通过，则允许该请求执行，否则将请求传给等级改变审核模块。等级改变审核模块依据系统等级改变审核策略检查是否能够通过临时改变或永久改变客体安全级的方式来允许该请求执行，如果可以，则允许该请求，否则拒绝该请求，同时进行审计报警。

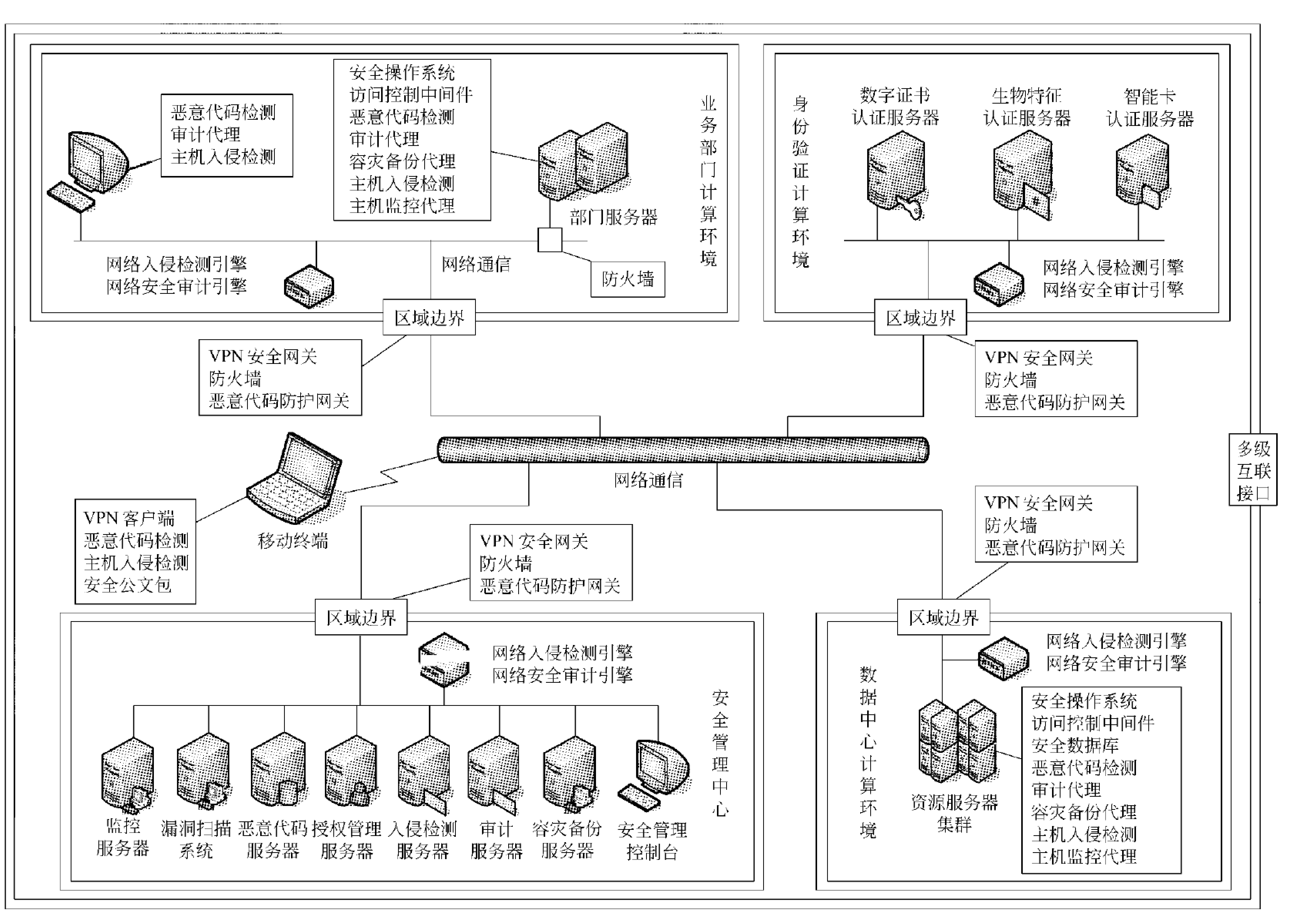



图 3-1　三级安全应用平台基本结构

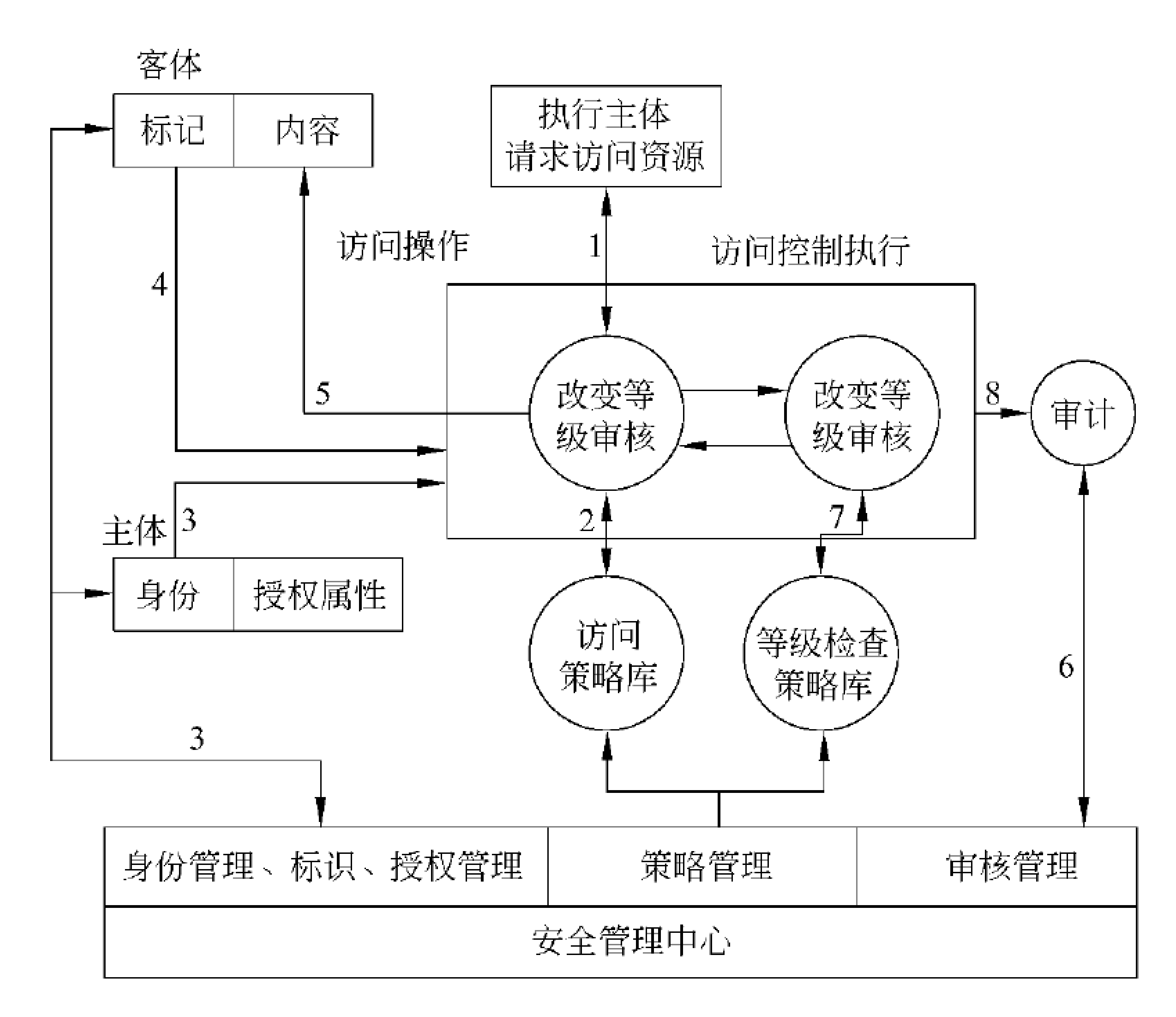



图 3-2　基于访问控制的总体结构流程

系统在使用之前，首先需要安全管理员对其进行初始化，即安全管理员通过安全管理中心制定系统安全策略（符合性检查策略、等级改变策略、自主访问控制策略等），确定系统中重要客体资源的安全级，确定系统中合法用户的安全级，确定系统中可用程序列表及其完整性摘要值，发行代表用户身份唯一标识的 USB-KEY 等。在此之后，安全管理员还需要对安全域中的所有终端、服务器、边界控制设备以及网络通信设备进行安全初始化，即确定所有平台的身份，确定平台操作系统内核的完整性状态等。

系统初始化完毕后，用户就可以安全地启动并登录系统。在此过程中，系统首先装载代表用户身份唯一标识的 USB-KEY，然后获取到 USB-KEY 中用户的信息，从而确定了系统的执行主体数据结构。在此基础上，系统请求策略服务器下载与该执行主体相关的系统安全策略，下载成功后，系统将初始化用户的执行空间，此后，用户便可以启动应用，访问系统中的信息资源。

系统中的应用代表用户行使权限，当应用发出访问本地或网络资源的请求后，系统中的强制访问控制模块将截获该请求，取出其中的主体、客体和操作信息，然后查询系统全局主客体表，得到相应主客体的安全级信息，以对其进行策略符合性检查，即检查该请求是否满足系统的安全策略，如果检查不通过，系统将依照等级改变策略对该请求进行异常处理，即判断发出该请求的主体是否有特权访问该客体，如果上述检查都不通过，系统将拒绝该请求，并进行审计处理。生成的审计信息将被送往审计服务器，供系统审计员检查。当上述检查通过后，该主体获得了访问对应资源的权限，但是如果请求资源和主体不在同一个安全域，那么该请求必然会将边界控制设备截获并且进行安全性检查。边界控制设备不仅接受本域安全管理中心的统一管理，而且需要上一层安全管理中心为其制定跨域的互联策略，这样安全管理中心就可以从跨域的角度检查是否允许该主体请求该客

体资源。当检查通过后，该请求包将通过安全的通信网络传到指定安全域中，在传输过程中，不会受到恶意的窃听和篡改。在系统被使用的过程中，有时会因为业务的需要改变主客体的安全级，这时需要用户向安全管理中心提出申请，安全管理中心接到申请后，将通知相关审批结构进行审核，如果审核通过，安全管理中心将为该主客体重新定级，生成新的主客体表，通知安全域中的节点设备同步。

## 3.2　实现方案和设备类型

根据强制访问控制的总体流程，可将三级安全应用系统分为七个子系统：网络通信安全子系统、区域边界安全子系统、计算节点子系统、应用访问控制子系统、典型应用子系统、安全审计子系统和安全管理子系统组合。其系统组成如图3-3所示。

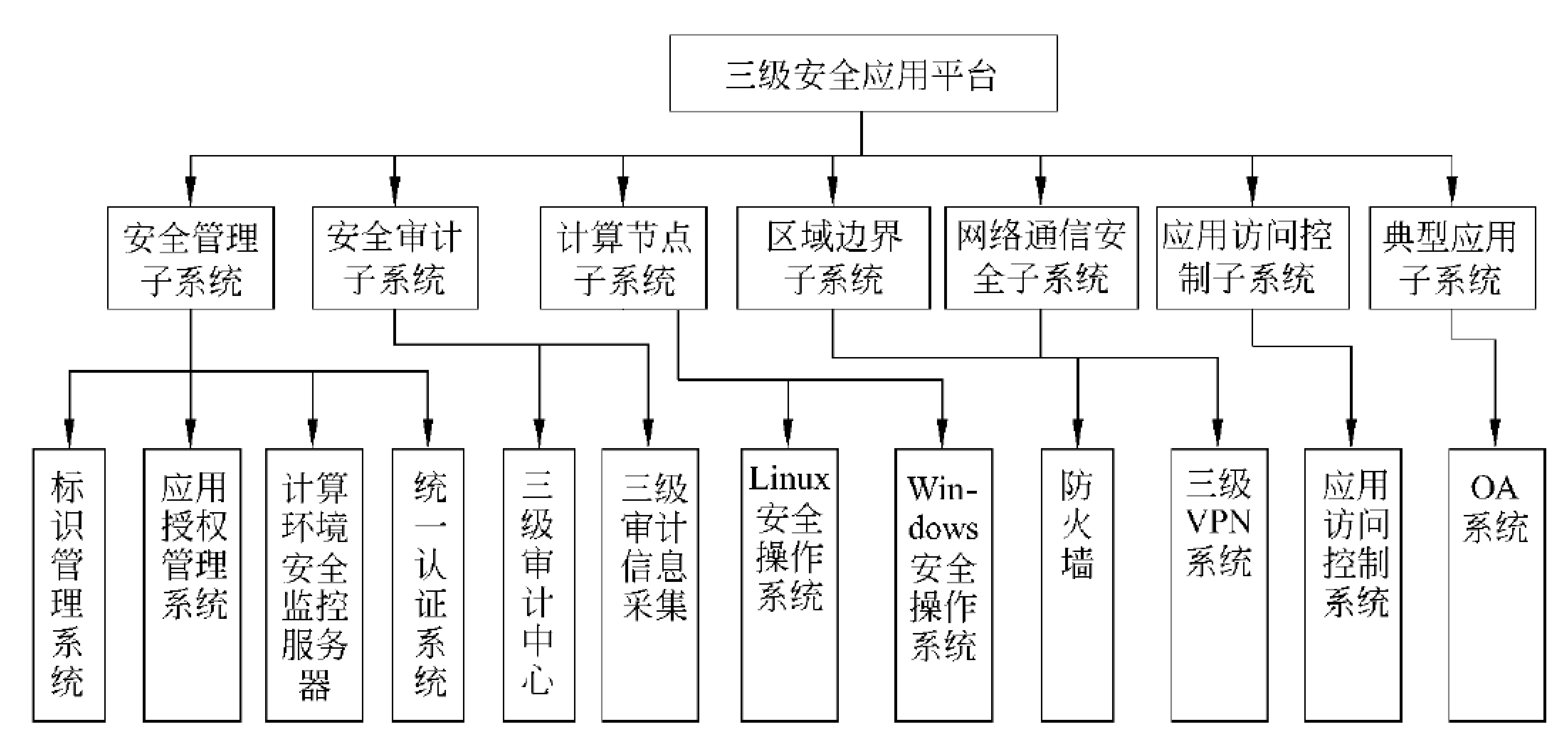



图3-3　三级安全应用系统组成

### 1. 网络通信安全子系统

网络通信安全子系统对安全域间的信息流进行封装，确保信息在传输过程中不会被非法窃听和篡改，主要由三级VPN系统组成。

### 2. 计算节点子系统

计算节点子系统对访问终端和服务器的系统进行增强，使其支持强制访问控制，由Windows安全操作系统和Linux安全操作系统组成。

(1) Windows安全操作系统

对现有Windows操作系统进行安全增强，如增加标识、强制访问控制、客体重用等安全功能，增强身份鉴别级别机制的安全性，部分实现系统的结构化，使其基本满足GB 17859的三级要求，为信息系统的安全提供有效支撑。

(2) Linux节点子系统

对Linux操作系统进行结构化改造和安全增强，如增加标识、强制访问控制、客体重用等安全功能，增强身份鉴别级别机制的安全性，明确系统核心层、系统层以及应用层的

边界，对各层之间的信息流进行安全检查，确保系统 TCB 始终有效、不会被恶意篡改，为上层应用系统的安全提供足够支撑。

### 3. 边界控制安全子系统

对流入或流出应用环境的信息进行安全检查，增强其强制访问控制功能，保护应用环境的安全性不会受到破坏，它由增强型防火墙组成。

### 4. 应用访问控制子系统

对应用资源进行授权管理并实施基于角色和安全标识的访问控制，防止应用系统资源被非授权访问，它由应用访问控制系统组成。

### 5. 安全管理子系统

对信息系统中的终端节点、边界控制、网络传输安全实施集中管理，包括管理用户和平台身份、标识主/客体安全等级和范畴、制定自主访问控制策略、符合性检查策略、等级改变策略、可信接入策略、系统可信预期值列表等，为三级信息系统的安全提供基础保障。

### 6. 安全审计子系统

对信息系统中的终端节点、边界控制、网络传输、安全管理统一实施与安全相关的审计管理，包括制定审计策略、接受并处理审计结果信息等，为判断系统安全状态提供依据。

### 7. 典型应用系统

典型应用系统的实现基于强制访问控制的模拟应用，在本项目中选用 OA 系统，模拟三级平台中的最常见的办公和公文处理。

## 3.3 安全计算环境子系统的设计和实现

### 3.3.1 系统设计

通过计算节点子系统来实现。具体的功能要求如下所述。

① 强制访问控制：三级 Windows 操作系统需支持二维标识模型的强制访问控制机制，能够保护信息系统的机密性及完整性不受破坏。强制访问控制机制的实施与系统二维安全模型一致的安全策略能够控制进程对文件的所有操作。强制访问控制机制始终有效，不会被旁路。

② 标记：三级 Windows 操作系统需对系统中的进程、文件进行全程标记，确保主客体在整个生命周期中其标记信息都是准确完整一致的。其提供三维标记，标记实体保密性级别、完整性级别和范畴。标记的对象包括系统中的用户、所有文件及进程。能够确保实体在整个生命周期中，其标记信息是准确完整一致的。

③ 身份鉴别：三级 Windows 操作系统应有基于可信硬件设备的安全身份鉴别机制，且可以通过安全的机制将身份与授权权限绑定。能够提供基于可信硬件设备的安全身份鉴别机制，确保非授权用户无法访问信息系统。

④ 审计：三级 Windows 操作系统应能对系统中所有违反安全策略的操作进行审计，并能阻止非审计管理员用户对审计信息的访问或破坏。能够记录下述事件：用户登录事件、客体的创建和删除事件、安全管理员、安全审计员、系统操作员以及系统中其他用户的一切与安全相关的行为。审计的具体内容以满足 GB 17859—1999 中三级系统的审计规范要求为标准。

⑤ 数据完整性：三级 Windows 操作系统可通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。

## 3.3.2　系统实现

为了实现前面所述的安全功能，不仅需要对现有的 Windows 操作系统平台进行安全增强，而且需要针对特殊的应用，对其进行安全封装，以使其满足高等级的安全需求。图 3-4 是三级Windows 操作系统中各安全模块之间的关系图。

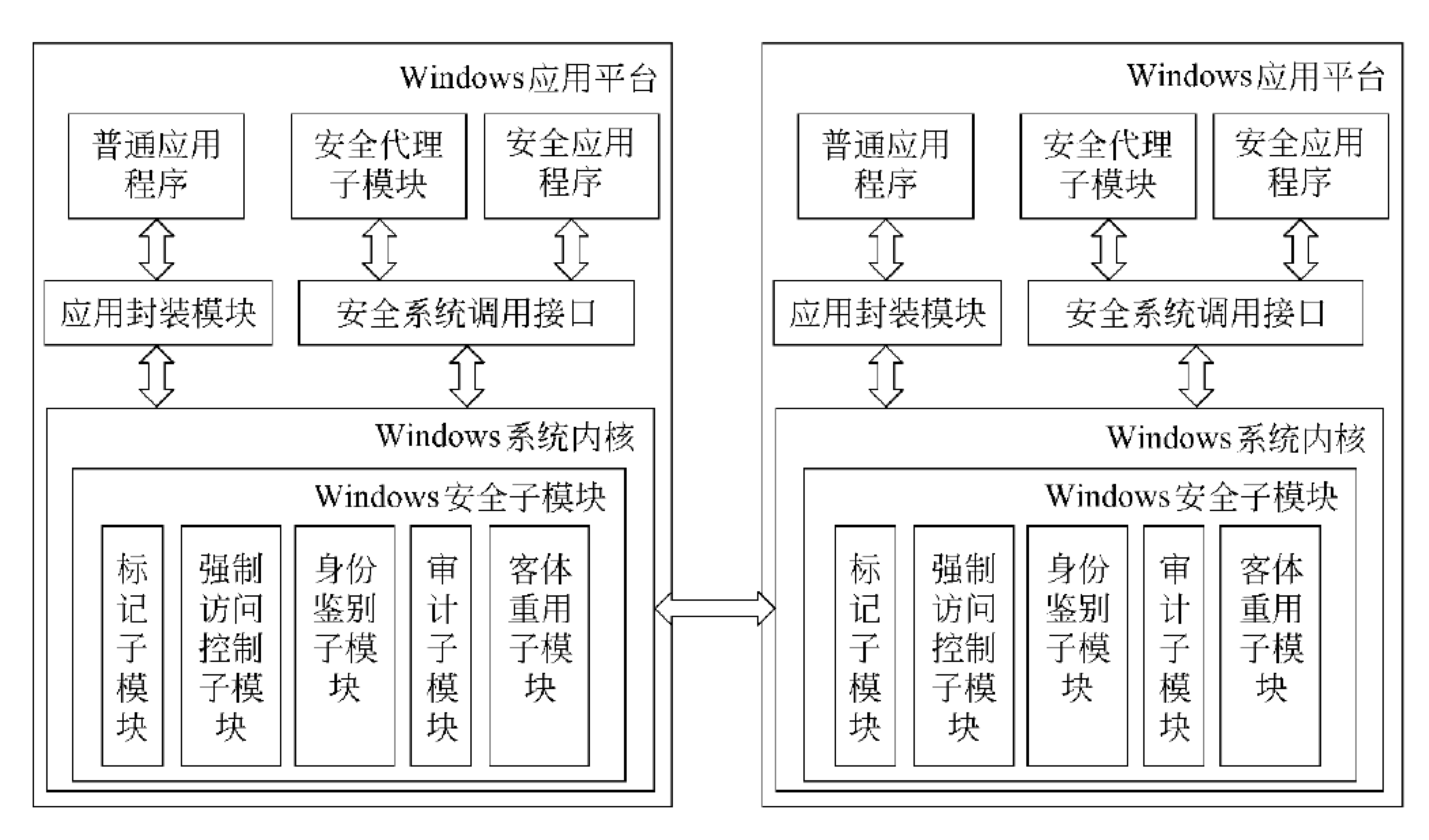



图 3-4　三级 Windows 操作系统子模块关系

由图 3-4 可以看出，Windows 安全子模块是三级 Windows 操作系统安全的核心，负责实现大部分的安全功能，包括标记、强制访问控制、身份鉴别、审计以及客体重用等；应用封装模块负责对现有的应用程序进行安全封装，使得系统的安全机制能够捕获应用运行时的语义，从而能够更灵活地进行诸如访问控制等系统安全决策，确保在不破坏系统安全性的前提下更好地支撑上层安全应用；安全系统调用接口是三级 Windows 操作系统在现有操作系统基础上封装出来的一系列安全系统调用，使得安全应用程序能够通过调用这些接口将应用的语义传递给操作系统，方便操作系统进行安全决策；安全代理子模块是一个系统服务程序，负责和安全管理中心及其他终端平台之间的信息交互，包括标记信息的同步、安全策略的同步、可信证明的信息交互等。下面将详细描述上述各模块的工作流程、相关数据结构以及模块之间的接口关系等。

### 1. 标记子模块工作流程

标记子模块主要为强制访问控制模块提供标记管理服务，包括获取主体标记、获取客体标记、临时修改客体标记、永久修改客体标记等。当标记管理模块收到上述请求后，将访问存放在本机上的标记库，从而做出相应的动作。由于安全域中用户的数量有限，所以三级 Windows 操作系统平台中的主体标记库是全局一致的，由安全管理中心统一分发和管理，即当有用户信息发生改变时，安全管理中心将发出命令，要求安全域中的所有终端到安全管理中心去同步该修改信息。然而，由于信息系统的复杂性，客体的数量极其庞大，因此三级 Windows 操作系统平台的客体标记库是局部的，只包含本终端上的所有文件的客体标记，当访问控制模块请求其他终端上的客体标记信息时，标记子模块需要通过安全代理程序和对方终端通信，以请求对方的标记子模块返回相应的客体标记。

### 2. 强制访问控制模块结构和工作流程

强制访问控制工作流程如图 3-5 所示。

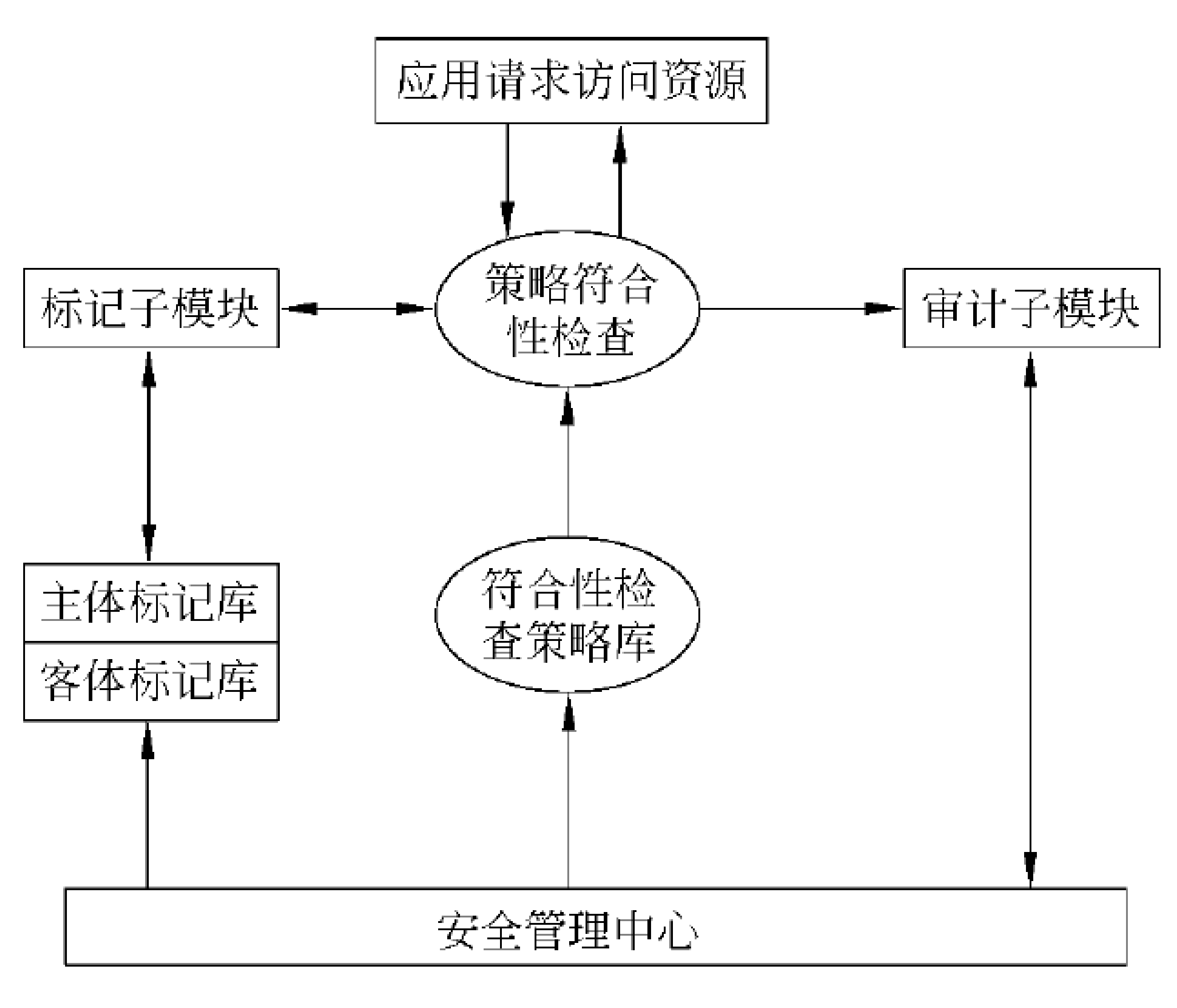



图 3-5　强制访问控制工作流程

应用发出访问请求后，操作系统强制访问控制模块会拦截到该请求，并对其进行策略复合性检查。但是为了检查该访问请求是否符合系统安全策略，访问控制模块需要与标记子模块通信，以获得访问请求中主客体的安全标记。在此基础上，强制访问控制模块依据系统符合性检查策略判断该请求是否安全，如果检查通过，则允许该请求执行。

然而在现有 Windows 计算平台上，从应用层到操作系统层，再到设备层，操作被逐步细化，随之而来的是操作所在的语境被逐渐冲淡。例如在操作系统层只能看到基本的读、写、创建、执行等动作，但是这些动作是在什么语境下发起的，相关应用的流程如何，操作系统层并不得而知，于是会出现应用层某个安全合理的请求，在操作系统看来就是不安全的情况。因此，仅仅在操作系统层进行访问控制，难免会出现控制不灵活，影响系统可用性的情况。为了解决以上问题，本项目采用图 3-6 所示的强制访问控制架构，充分结合应用的流程，在具体应用语境下判断应用操作请求的安全性，实用性更强。

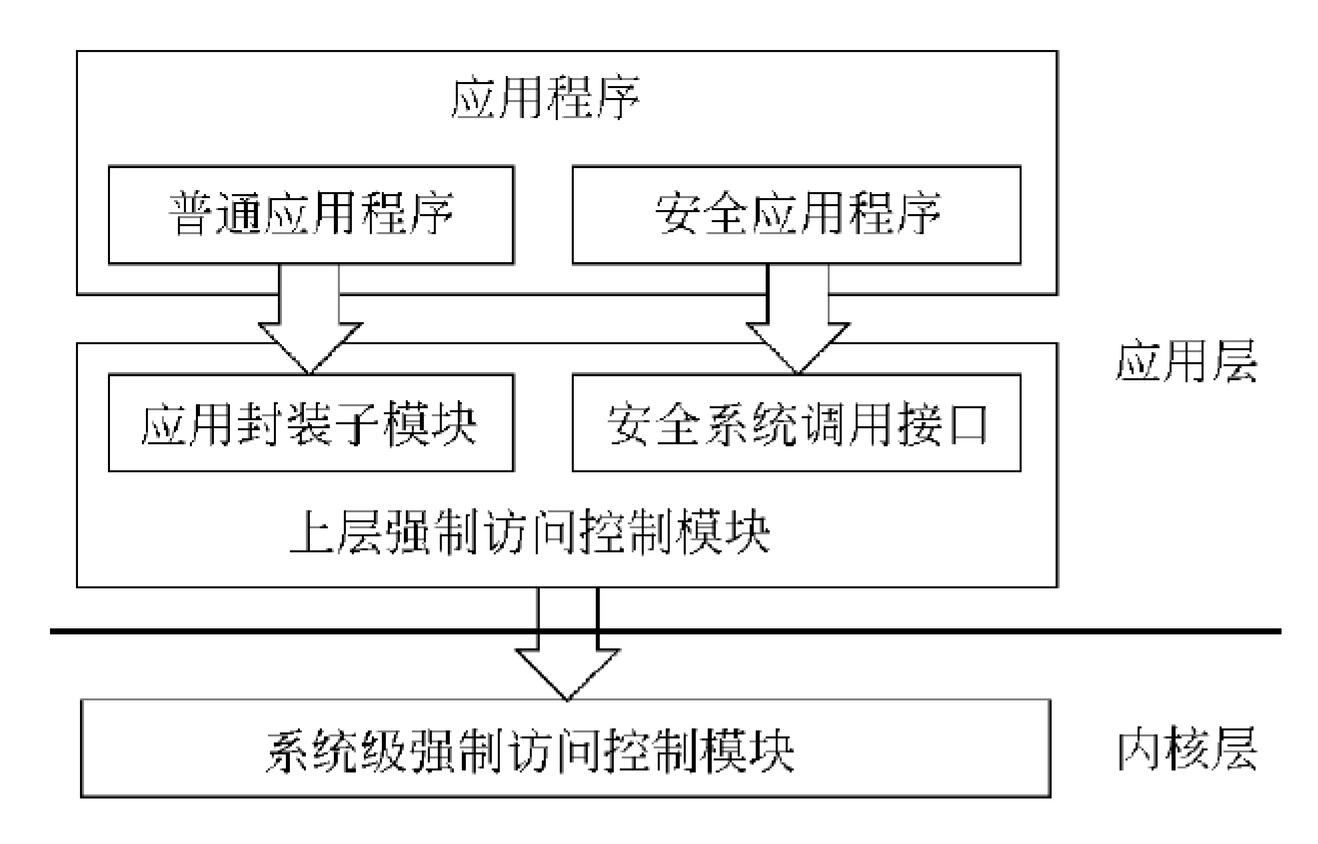



图 3-6　强制访问控制模块架构

由图可以看出，本项目中的强制访问控制模块被分成两层，底层是系统级的，这一层只能看到操作系统级的一些基本动作，也只能严格按照安全模型进行强制访问控制，对出现违背安全策略的操作缺乏结合应用流程进行安全检查的能力。上层强制访问控制模块能够充分结合应用的流程，作出更准确实用的强制访问控制决策。由于实现方式不同，上层强制访问控制模块被分成两种：安全封装和安全系统调用接口方式。其中安全封装方式适用于那些已经成熟的或源代码不可控的关键应用，通过拦截这些应用发出的系统调用，还原出相应的应用流程信息，以便在应用发出违背系统安全策略的请求时，对其进行调节，以满足业务的正常需求。安全系统调用是一些经过安全封装的系统调用接口，内嵌强制访问控制机制。对接口进行封装的目的是确保应用相关的流程及语境信息能够传递到强制访问控制模块中，从而使得强制访问控制模块能够利用这些信息进行策略符合性检查和等级改变检查，最终作出更合理的访问控制决策。

### 3. 身份鉴别模块流程

身份鉴别分为用户身份鉴别和平台身份鉴别两种，在现有的 Windows 操作系统中，这两种身份鉴别机制都比较薄弱。如 Windows 操作系统采用单一口令的方式对用户进行身份鉴别，这种方式容易遭受字典攻击；而以 Windows 操作系统为基础的终端在相互通信时，并没有验证对方平台身份的环节，容易遭受平台身份假冒攻击。因此，在三级 Windows 操作系统平台中，应对上述两种身份鉴别机制进行安全增强，确保非授权用户无法入侵信息系统。

针对用户身份鉴别，三级 Windows 操作系统增加了一个硬件模块 USB-KEY，作为用户身份的唯一标识，当用户登录系统时，需要插入 USB-KEY，然后操作系统对用户进行双因子身份认证，只有用户拥有合法的 USB-KEY，并且输入正确的 Windows＋USB-KEY 口令，才能登录系统。

针对平台身份鉴别，三级 Windows 操作系统要求在平台收到其他平台发出的连接请求时，都要鉴别对方的平台身份，确保只有合法可信的平台能够和其进行相互通信。其工作流程如下：平台收到其他平台的连接请求后，将通知安全代理程序模块获取对方的平台身份，安全代理模块接到请求后，将主动和对方的安全代理程序模块通信，请求对方平台的身份，然后将得到的身份返回给身份鉴别模块，身份鉴别模块验证其可信性。

#### 4. 审计模块流程

审计模块的作用是依据安全管理中心制定的审计策略，记录平台上用户的相应操作行为，尤其是用户违背系统安全策略的行为。显然，审计模块需要和系统中的其他安全功能子模块（如标记子模块、访问控制子模块或身份鉴别子模块等）进行通信，以明确用户的操作行为及相应安全机制作出的决策结果。当审计模块收到这些安全功能模块发出的信息后，将对照系统的审计策略，确定需要对什么样的动作进行审计，需要记录相应动作的什么信息等，从而形成审计日志。为了安全管理的需要，终端上的安全代理程序需要定期地将本地的审计日志上传到安全管理中心，存放到审计信息库中，使得安全管理员可以从中了解各终端的运行状态，并且在发生安全事故后，可以寻找元凶，如图 3-7 所示。

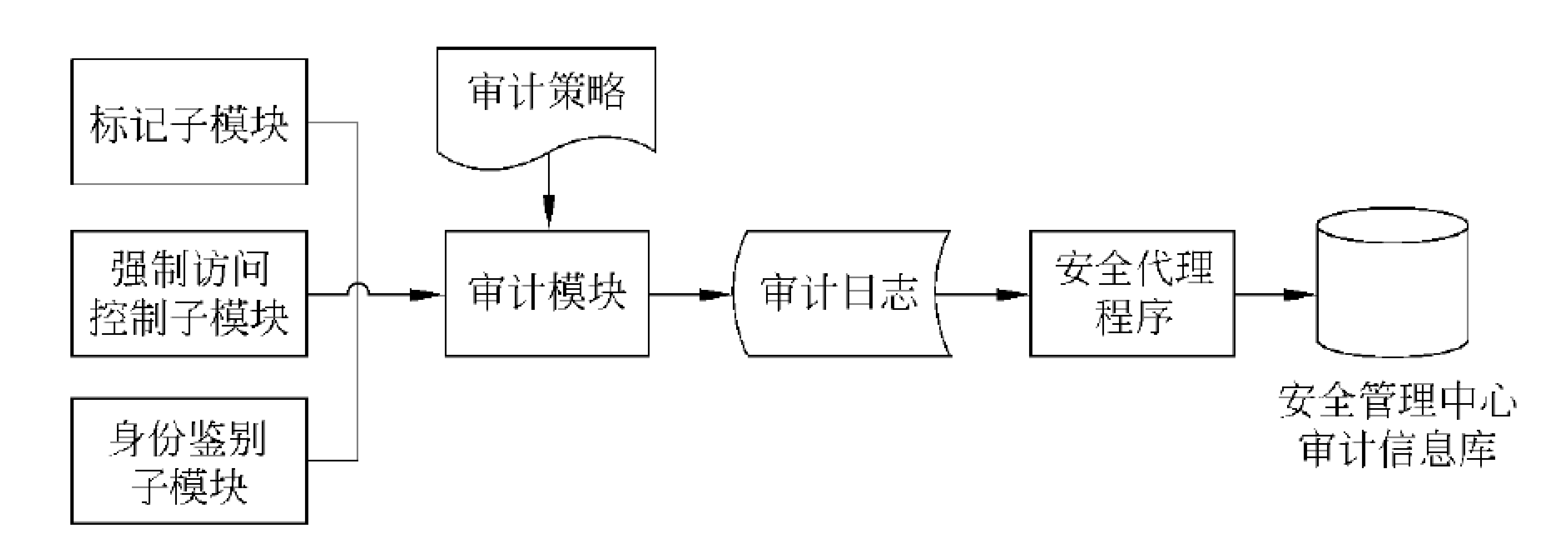



图 3-7　审计模块工作流程

#### 5. 主要数据结构

有以下四种：

(1) 安全标记数据结构；

(2) 主体安全标记数据结构；

(3) 客体安全标记数据结构；

(4) 客体临时安全标记数据结构。

#### 6. 接口设计

(1) 标识管理模块提供服务接口

当访问控制模块接到这一请求后，会依据等级改变审核策略，判断是否允许该主体对该客体的安全级作如此改变，如果允许，则请求标识管理模块作相应修改，否则拒绝该请求。

(2) 强制访问控制子模块接口

① 安全打开文件接口。安全系统调用接收到这一访问请求后，需要根据入口参数 SubLable 结构向安全标记子模块请求发起该操作的主体安全标记，同时根据 FileName 获得客体安全标记，然后请求系统打开该文件。如果打开成功，则安全调用接口将记录主体安全标记、客体安全标记以及文件句柄供以后的访问控制用，然后返回文件句柄给上层应用。

② 安全读文件接口。安全系统调用接收到这一访问请求后，将查找内部维护的和该文件句柄相关的数据记录，以获取到打开该文件的主体安全标记以及该文件的客体安全

标记，然后依据符合性检验策略判断该主体是否能够读操作该客体，如果不能，则检查等级改变策略，看是否能够临时改变客体的安全级，以允许该行为发生。

③ 安全写文件接口。安全系统调用接收到这一访问请求后，将查找内部维护的和该文件句柄相关的数据记录，以获取到打开该文件的主体安全标记以及该文件的客体安全标记，然后依据符合性检验策略判断该主体是否能够写操作该客体，如果不能，则检查等级改变策略，看是否能够临时改变客体的安全级，以允许该行为发生。

## 3.4 安全区域边界子系统的设计和实现

### 3.4.1 系统设计

安全区域边界子系统的实现基于主客体标识的访问控制。其控制目标为：定义网络环境下主体与客体的内涵，对主体与客体进行安全标记；以安全管理为手段，建立边界访问控制策略；以主体与客体的安全级为基础，实施网络边界的强制访问控制，提供基于用户的强制接入控制和边界强制访问控制等功能；通过以安全标记为基础的安全审计，保证强制访问控制的可核查性；同时提供数据机密性、完整性等机制，保证信息的安全传输。网络边界子系统的边界控制功能与 VPN 功能一体化实现在相同的控制点进行控制，保证传输安全性的同时，提高了网络数据包处理效率。

安全区域边界子系统作为置于不同网络安全域之间的访问控制设备，一般安装在计算环境的交界上，具有基于安全标记的过滤和管理进出数据包、封堵禁止的访问行为、记录通过防火墙的信息内容和活动、对网络攻击进行检测和告警、阻止非法访问等功能。

为实现以上的安全功能，区域边界子系统主要包括包过滤模块、内容过滤模块、流量统计与控制模块、网络审计模块、应用代理模块和 Qos 管理模块等组成部件。

#### 1. 基于安全标记的数据过滤模块

基于安全标记实施非法接入和网络访问控制。

#### 2. 包过滤模块

对数据包实施基于策略的过滤，支持用户自定义的安全策略。安全策略可以是 MAC 地址、IP 地址、端口、协议类型和时间的部分或全部组合。安全策略使用最小安全原则，即除非明确允许，否则就禁止。

#### 3. 网络地址转换

实现 NAT、SNAT、DNAT 等网络地址转换，并与安全标记相结合，实现地址转换后的标记绑定。

#### 4. 网络审计功能模块

提供全面、细致的日志记录及良好的日志分析能力，支持生成审计报表，确保只有合适的管理员才能管理审计日志。

### 3.4.2 系统实现

#### 1. 出包处理流程

当网络数据包经过防火墙外出时，首先提取访问源和目的安全标记，然后根据安全标记判断本次访问是否符合强制访问控制策略，如果不符合表示是非法外连，则丢弃数据包。如果符合策略，进行是否需要 SNAT 判断，若不需要，则直接发送，否则进行网络地址转换后发送。

#### 2. 入包处理流程

当网络数据包经过防火墙接入时，首先提取访问源和目的安全标记，若是远程接入用户，则根据用户的安全标记，判断是否符合接入控制策略，若不符合表示本次访问是非法接入，则丢弃数据包。允许接入则进行基于源、目的安全标识的强制访问控制策略判断，如果符合策略，就进行是否需要 NAT 判断，若不需要，则直接发送，否则进行网络地址转换后发送。

#### 3. 审计模块工作流程

审计模块的作用是依据审计策略记录数据包的操作行为，尤其是违背系统安全策略的行为。对照系统的审计策略，确定需要对什么样的行为进行审计，需要记录相应行为的什么信息等，从而形成审计日志。为了安全管理的需要，防火墙的安全代理程序需要定期地将本地的审计日志上传到安全管理中心，存放到审计信息库中。

#### 4. 主要数据结构

有以下五种：

(1) 网络表数据结构；

(2) 端口列表数据结构；

(3) 地址表数据结构；

(4) 包过滤策略数据结构；

(5) 审计数据结构。

## 3.5 安全通信网络子系统的设计和实现

### 3.5.1 系统设计

安全通信网络子系统的组成结构主要包含过滤与核心总控模块、安全隧道处理子系统、自主访问控制子系统、强制访问控制模块、基于用户的审计子系统、安全管理代理、认证代理以及维护的安全数据库等组成部件，其组成结构如图 3-8 所示。

① 过滤与核心总控模块：对经过 VPN 安全网关的数据流进行过滤，根据外出和进入分别进行相应地处理调度。

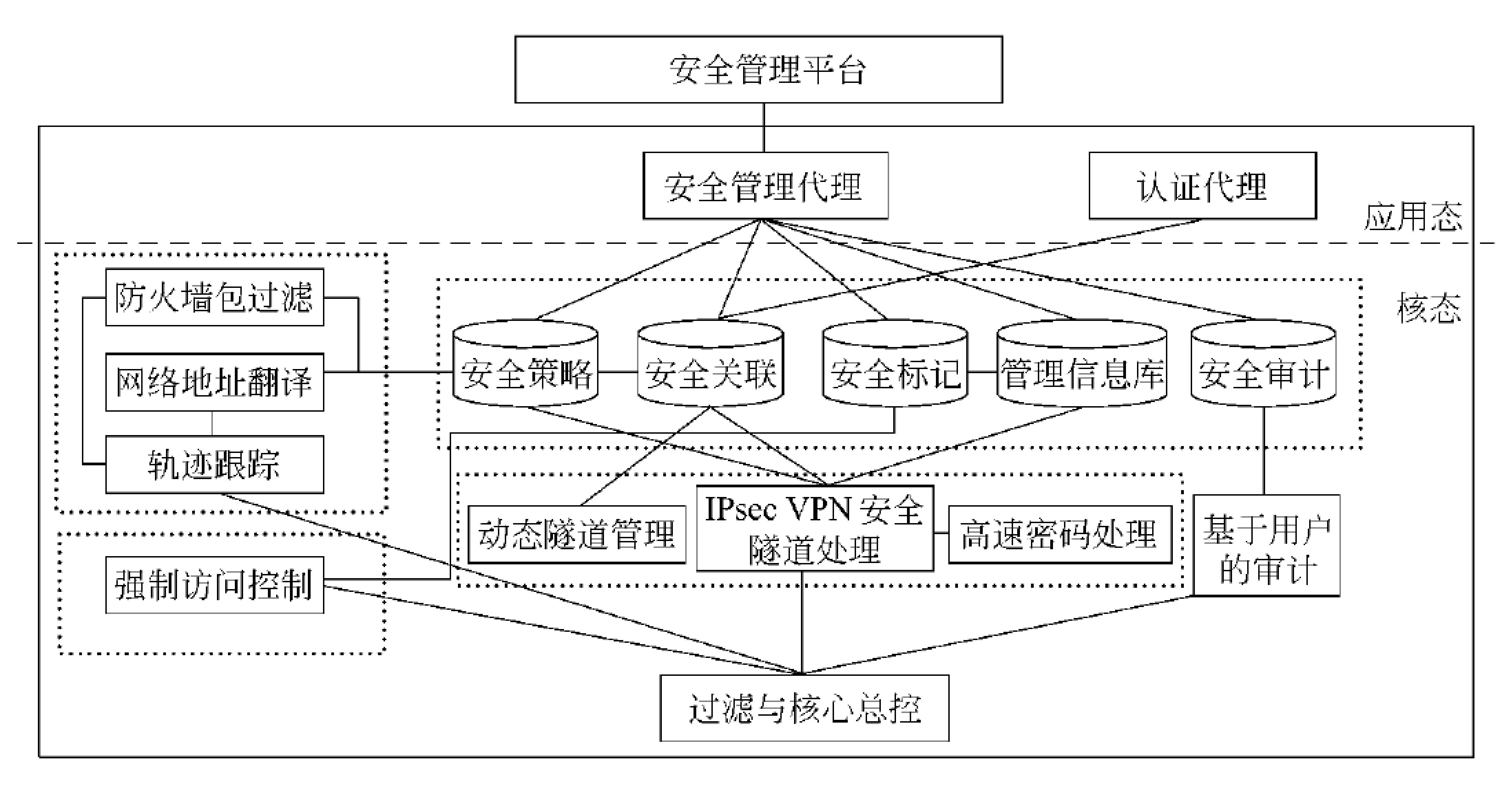



图 3-8　安全 VPN 安全网关组成结构

② 安全隧道处理子系统：由动态隧道协商模块、安全隧道处理模块、高速密码处理模块等组成。对于需要实施 VPN 隧道保护的信息流，从 SAD 检索保护该信息流的隧道安全参数等信息，调用高速密码处理模块，实施一体化的加解密、认证等快速密码处理，并进行封装等具体的安全隧道处理操作。

③ 自主访问控制子系统：包括防火墙包过滤、NAT 以及轨迹跟踪模块。防火墙包过滤与 NAT 的实现均建立在对数据报文的轨迹跟踪上，达到基于状态包检测的数据包过滤功能，以及网络地址转换功能。

④ 强制访问控制模块：通过提取数据流中的安全标记以及查询管理信息库得到主客体的安全级和范畴集，通过对主客体的安全级和范畴集进行比较实施访问请求的合法性判断。

⑤ 安全审计子系统：根据安全审计策略，对正常网络信息流及处理情况按用户和地址进行审计，对违规事件、网关运行状态和管理情况进行审计并分类存储。

⑥ 管理代理模块：是边界强制访问控制系统与安全管理系统进行交互的唯一接口。其具体功能包括安全策略管理、隧道管理、审计管理、安全标记管理以及网络实体对象管理等。

⑦ 认证代理模块：主要用于在网关启动里完成网关的认证和动态隧道建立过程中动态隧道的协商。

⑧ 安全数据库：包括安全策略数据库、安全关联数据库、安全标记数据库、管理信息库以及安全审计数据库等组成部分。

安全 VPN 安全网关作为信息安全综合设备，具有边界防护、安全互联、信息加密、访问控制等功能。在三级平台下它应该达到的主要安全指标包括以下几项。

① 安全标记功能：VPN 安全网关负责对整个信息系统中的主体与客体进行安全标记。对接入内网的用户或发起连接的源地址进行安全标记绑定，对网关所保护的资源(如内网的 Web 服务等)进行安全标记，为基于用户安全标记级别的强制接入控制和基于网络数据流的边界强制访问控制打下基础。

② 基于网络数据流的边界强制访问控制：VPN 安全网关对负载访问请求的数据流实施基于安全标记的强制访问控制。网关从负载访问请求的数据流中提取出访问主体的安全级，与其所请求的目标资源安全级进行比较，根据预先设置的强制访问控制策略实施基于主客体标识的边界强制访问控制，从而保证信息系统的机密性不受破坏。

③ 基于用户的强制接入控制：VPN 安全网关根据预先设置的强制访问控制策略，通过用户的安全级为其分配相应的访问权限，通过对流入网关的数据流进行标记提取、权限判断等操作对发起连接的用户实施基于安全标记级别的强制接入控制，从而保证对违规用户的接入行为进行安全防范。

④ 基于用户的安全审计：VPN 安全网关对出入网关的网络连接实施基于用户的行为跟踪，从而实现对整个信息系统中所有违规操作的安全审计，并能阻止非审计管理员用户对审计信息的访问或任何破坏审计信息完整性的违规操作。

⑤ 身份鉴别：三级网络边界安全防护体系应提供基于可信硬件设备的安全身份鉴别机制，VPN 安全网关对于安全接入的移动用户进行基于数字证书的身份鉴别，以保证接入用户的合法性和可信任性。

⑥ 数据机密性和完整性防护：VPN 安全网关对数据源进行完整性校验，通过加密机制和隧道机制对所保护的数据进行机密性保护和有限的数据流机密性保护，从而保证业务数据流在网络边界的安全传输。

⑦ 分域防控：根据信息系统中的数据功能类型和敏感程度划分为不同的区域，通过 VPN 安全网关的不同接口进行物理隔离，对不同的安全区域实施基于敏感级的访问控制。

⑧ 基于网络对象的安全管理：网络实体包括用户、地址、子网、服务、接口等，在网络实体管理中引入对象的概念，用以标识具有相同安全特征值的网络实体。对网络中的网络实体进行基于对象的安全分组分类管理。提高边界访问控制系统中策略设置的易懂性，增强用户使用的透明性。

### 3.5.2 系统实现

#### 1. 出包处理流程

当网络数据包经过网关外出时，在过滤与核心总控模块的控制协调下，依次流经强制访问控制模块、自主访问控制子系统和隧道处理子系统等功能部件并进行相应的处理操作。具体的数据包处理流程如图 3-9 所示。

① 实施强制访问控制处理：当外出数据包流经安全 VPN 安全网关并经过过滤与核心总控模块进行流向识别后进入强制访问控制处理模块。强制访问控制模块通过检索管理信息库查找数据流所属的网络实体，根据网络实体的对象名查找安全标记数据库，得到该数据流主体的安全标记，将其写入数据流并发送至自主访问控制处理子系统进行下一步处理。

② 实施自主访问控制处理：自主访问控制子系统对接收到的数据流识别其状态信息、IP 信息、端口信息等特征，根据自主访问控制策略判断数据流是否允许外出。如果允许该数据流外出，则将其发送至 VPN 安全隧道子系统；如果不允许该数据流外出，则将

数据包丢弃。如果允许外出的数据流所对应的自主访问控制策略为 NAT 策略，则对数据流进行网络地址转换，然后发送至 VPN 安全隧道处理。

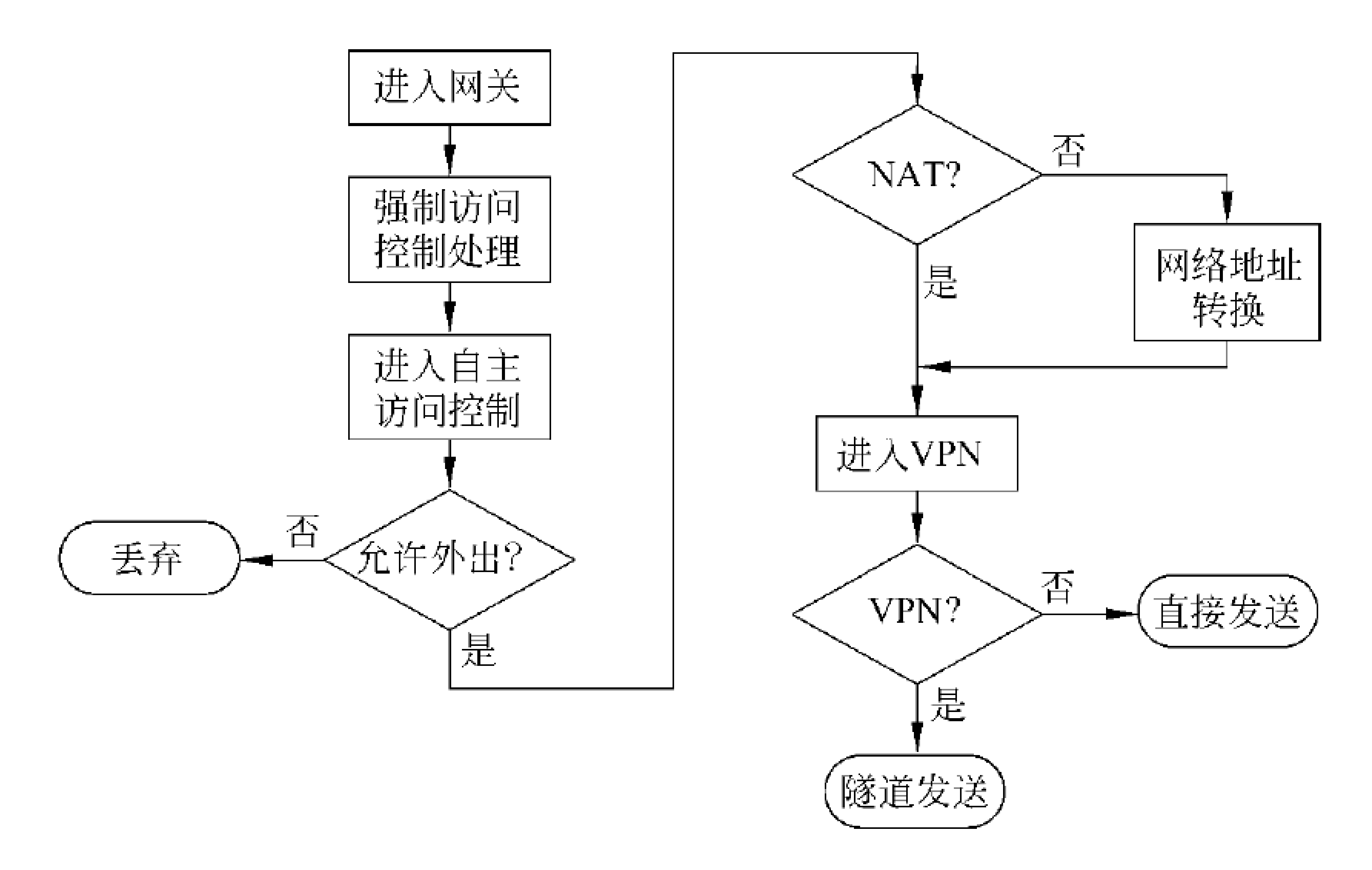



图 3-9　安全 VPN 安全网关出包工作流程

③ 实施 VPN 安全隧道处理：当数据包进入 VPN 安全隧道处理子系统时，首先通过检索管理信息库查找到数据流所对应的源和目标对象，根据对象与策略的对应关系查询 SPD，从而判断数据包进行 VPN 隧道处理的必要性。对于不需要进行 VPN 隧道处理的数据包专题报道发送；如果此数据包需要进行 VPN 处理，则通过查找 SAD 数据库获取安全隧道参数，然后在安全隧道处理模块和高速密码处理模块中对数据流进行封装、加密与认证处理，通过所建立的安全隧道发送。

## 2. 入包处理流程

当网络数据包从外网经过网关进入时，则在核心和过滤总控模块的协调下，依次流经隧道处理子系统、自主访问控制子系统和强制访问控制模块等功能部件并进行相应的处理操作。具体的数据包处理流程如图 3-10 所示。

① 实施 VPN 安全隧道处理：当数据包达到网关时，首先判断此数据包是否为 IPSec 数据包。如果该数据包不是 IPSec 数据包，则直接发送至自主访问控制子系统；如果该数据包是 IPSec 数据包，则进行相应的 IPSec 数据包处理流程，具体的处理过程如下所述。

首先根据 IPSec 报头信息(spi、目标地址等)查找 SAD 数据库。对于找不到相应 SA 的数据包实施丢弃操作；如果找到对应的 SA 则对数据包进行解封装、解密、认证等处理操作。然后对解封装后的数据包根据报头信息查找管理信息库，得到数据包所属的网络实体对象，进而根据对象名查找安全策略数据库 SPD，如果找到的安全策略不为 VPN，则丢弃此数据包，如果安全策略为 VPN，则允许数据包进入自主访问控制子系统。

② 实施自主访问控制处理：当数据包进入自主访问控制时，根据数据报头信息得到此数据包的自主访问控制策略，根据自主访问控制策略确定对数据包的下一步操作，对于策略为通过或丢弃的数据包进行相应操作；对于自主访问控制策略为 NAT 的数据包，则进行网络地址转换后发送至边界强制访问控制模块。

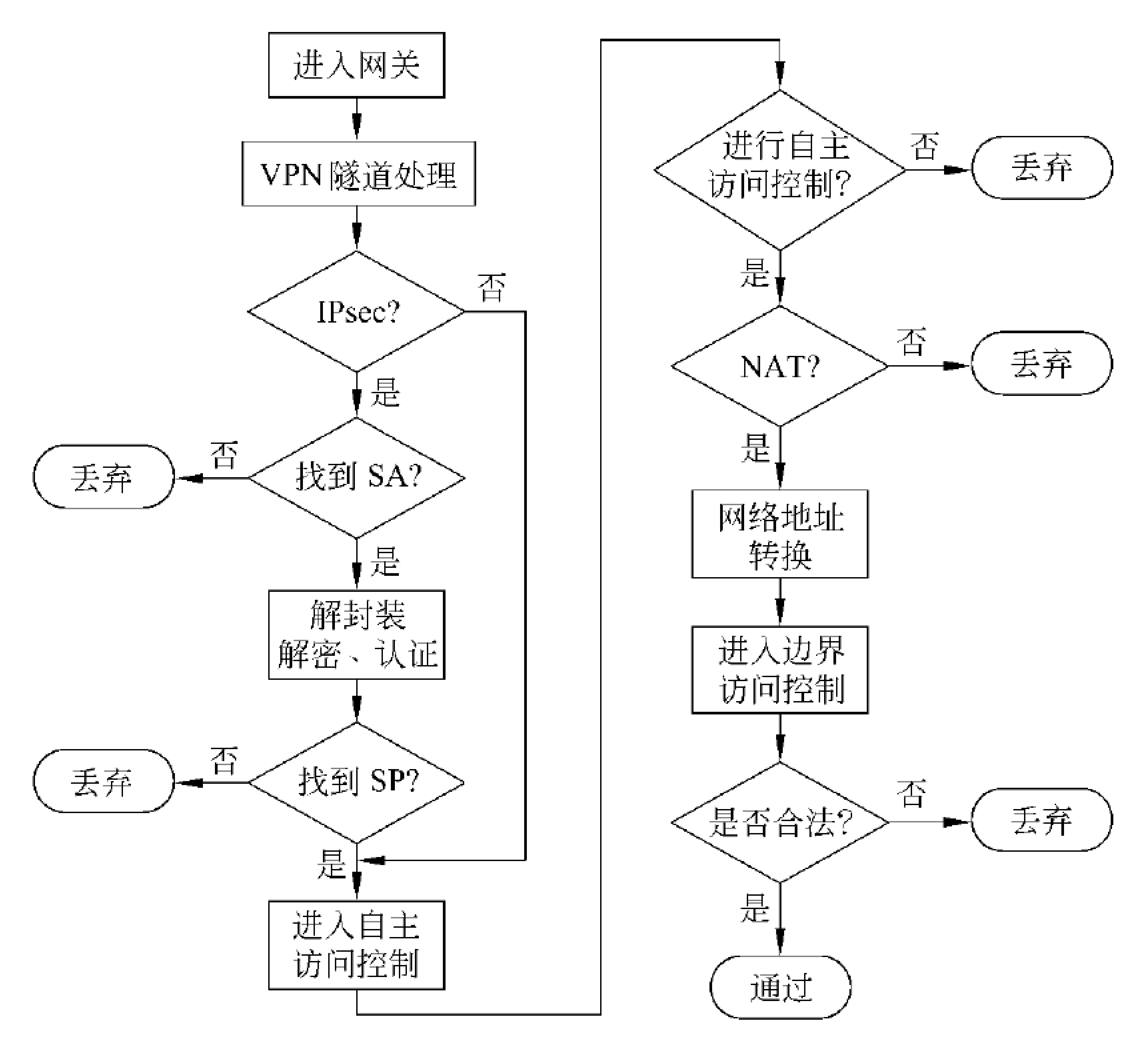



图 3-10 安全 VPN 安全网关入包工作流程

③ 实施强制访问控制：强制访问控制模块根据流入的数据包报头信息查找管理信息库，得到其所对应的对象名，据此检索安全标记数据库，得到目标客体的安全标记，并与数据包携带的安全标记进行比较，如果满足强制访问控制策略的要求（主体安全级≥客体安全级，且主体范畴集包含客体范畴集），就允许请求数据包通过，反之，允许响应数据包通过。

### 3. 主要数据结构

有以下三种：

(1) VPN 数据结构；

(2) 包过滤策略数据结构；

(3) 安全标记数据结构。

### 4. 接口设计

在 IP-VPN 安全网关内核中，提供了通用的加/解密、MAC 产生和认证调用接口，通过该接口完成对专用加密卡的驱动，为隧道的加/解密、完整性认证提供服务。

## 3.6 安全管理子系统的设计和实现

### 3.6.1 系统设计

安全管理子系统对信息系统中的终端节点、边界控制、网络传输安全实施集中管理，

包括管理用户和平台身份、标识主/客体安全等级和范畴、制定自主访问控制策略、等级改变策略、可信接入策略、系统可信预期值列表等，为三级信息系统的安全提供了基础保障。

根据对三级标准的理解，面向三级信息系统的安全管理子系统应提供如下三个功能。

① 能够为主体、客体分别分配统一安全标记（分别指定安全级和范畴集），并将主体、客体及其安全标记进行统一安全管理，可以根据相应的等级改变策略对实体的标记进行相应修正，使强制访问控制更易于实施。

② 参照用户信息和资源信息，为用户授予访问资源的权限，形成自主访问控制列表。

③ 制定安全策略，包括自主访问控制策略、等级改变策略等。

三级安全管理子系统主要由安全标记管理模块、策略管理模块、授权管理模块组成，如图 3-11 所示。

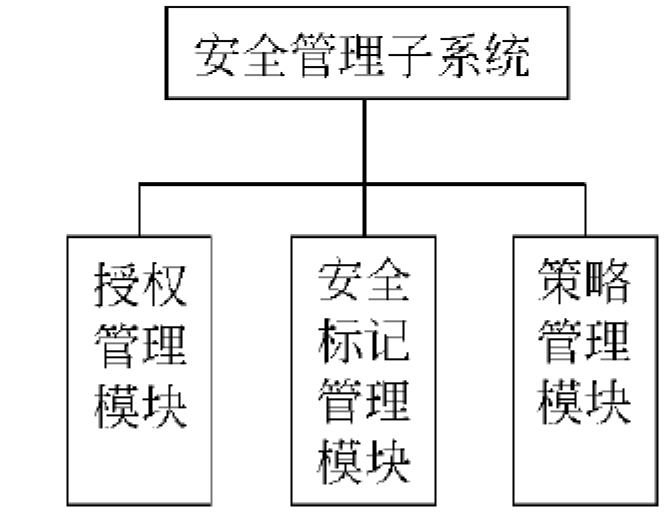



图 3-11　安全管理子系统的组成

### 3.6.2　系统实现

#### 1. 安全标记管理模块的工作流程

主体通过认证后，安全标记管理模块根据主体的权限和角色确定主体的安全标记，生成全局主体标记列表，同时根据客体的重要程度，确定所有客体的安全标记，生成全局标记列表，建立安全标记数据库和信息数据库。如果根据需要要永久改变客体的安全标记时，可以根据相应的等级改变策略对实体的安全标记进行相应修正。

#### 2. 策略管理模块的工作流程

策略管理模块根据安全需要制定自主访问控制策略、等级改变策略、可信接入策略等，并进行策略的维护工作，包括修改、更新和撤销策略等。只有安全管理员才可以对策略进行操作。

#### 3. 主要数据结构

包括以下两种：

(1) 安全标记数据结构；

(2) 客体临时安全标记数据结构。

## 3.7　审计子系统的设计和实现

### 3.7.1　系统设计

根据对三级标准的理解，面向三级信息系统的安全审计子系统应提供如下几个安全机制和功能。

#### 1. 强制访问控制审计

实现系统、应用、网络边界强制访问控制审计数据的汇总。

### 2. 网络数据流审计

对网络通信进行全面监测记录，提供对不同网络协议、网络应用程序的运行记录，实现对网络行为的重放功能。

### 3. 系统操作审计

对网络系统中的主机进行全面监测，监测内容主要包括主机运行过程中的安全事件如操作系统本身事件、用户行为、文件操作等记录。

### 4. 审计日志分析功能

安全审计应可以根据记录数据进行分析，提供对网络及主机运行状况的预测，对潜在用户异常行为及网络攻击事件进行预警，并生成审计报表。

### 5. 审计日志保护

安全审计提供基于角色的访问控制机制，以保证安全审计记录不会受到未预期的删除、修改或覆盖等。

### 6. 告警

安全审计提供系统审计记录的分类分级，对特定事件提供邮件、声音、文本等可定制方式的实时报警。

三级安全审计系统采用控制台/服务器/代理(Client/Server/Agent) 三级架构，主要由管理控制台、审计服务器和审计代理三部分组成。

## 3.7.2 系统实现

三级安全审计子系统实现对所辖系统中各应用系统安全事件的采集、存储与管理，为安全事件取证及安全管理人员决策提供支持。三级安全审计系统的详细工作流程如图 3-12 所示。

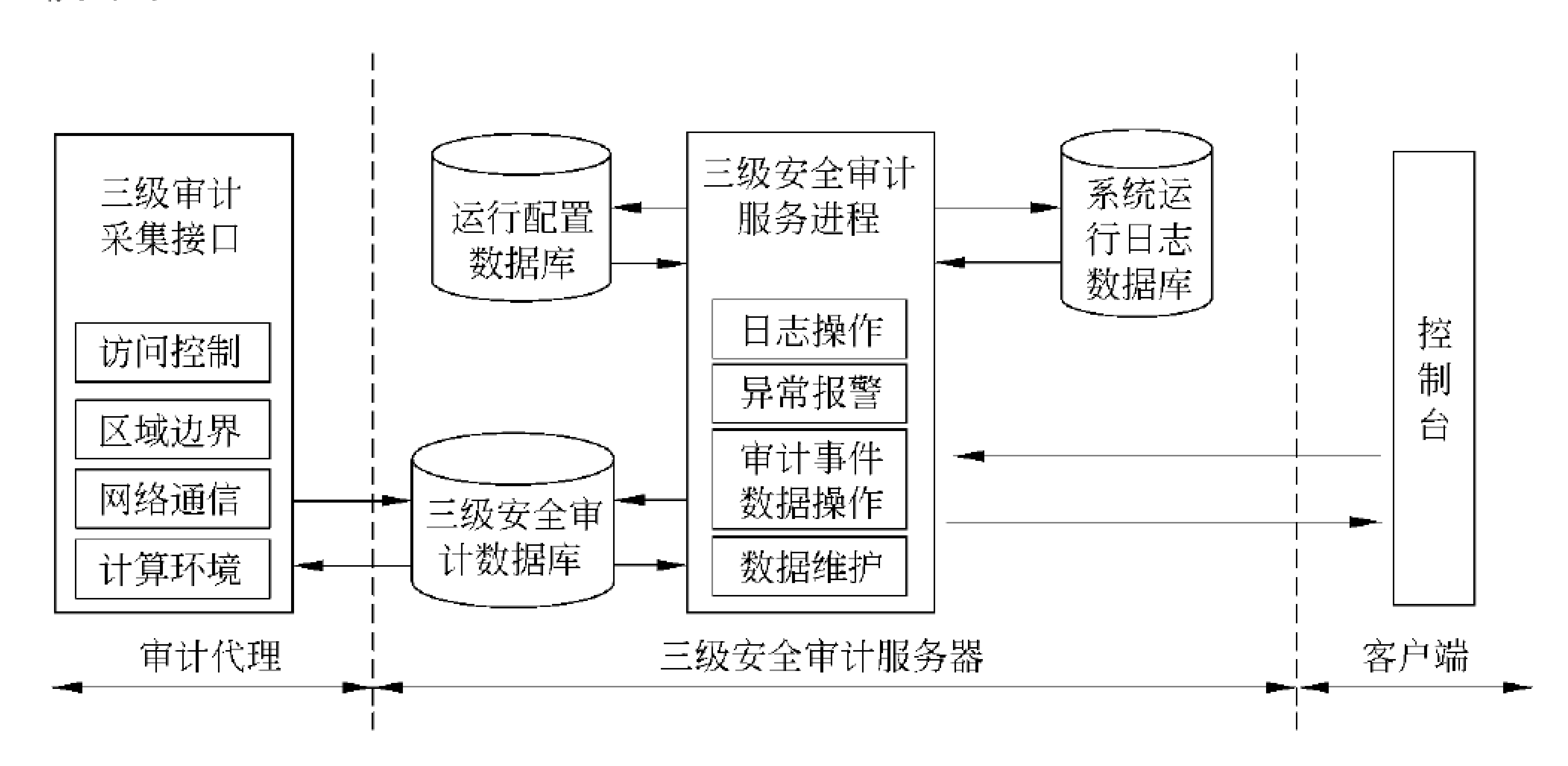



图 3-12 三级安全审计系统工作流程

其详细工作流程如下所述。

① 由强制访问控制子系统产生相关的访问控制审计数据，根据三级安全审计服务器

发布的数据采集策略，将审计日志数据写入服务器端的数据库中；基于主机的审计代理采集主机运行日志发送至服务器。

② 三级安全审计服务器通过与安全事件审计数据库进行交互，实现三级安全审计数据的查询、统计及备份恢复等操作；通过审计数据分析，得到三级审计主体可能的异常访问趋势，并提供异常报警信息；根据控制台的指令实现数据的备份与恢复。

③ 安全事件审计服务器根据运行配置数据库的配置信息，实现与数据库的连接，保证系统正常稳定运行。

④ 安全事件审计服务器记录本系统产生的各项操作日志，并将数据存储至运行日志数据库，根据控制台的指令实现对本系统日志的查看与管理功能。

⑤ 用户通过控制台发布操作指令，安全事件审计服务器执行指令并将执行结果返回给控制台。

### 1. 主要数据结构

它有以下两部分：

(1) 审计数据结构；

(2) 系统日志数据结构。

### 2. 异常行为模式数据结构

由于系统涉及用户较多，因此用户行为模式也各不相同。如果对采集到的大量安全审计数据不进行有效地统计和分析，就很难发现系统运行时用户的正常行为模式，无法判断当前用户行为是否偏离正常模式，从而无法对用户异常行为作出检测和及时响应。

数据挖掘的用户行为模式提取技术能够对海量安全事件审计数据进行探索，对审计数据进行关联分析和处理。关联规则能够有效地挖掘出审计数据集中不同属性字段之间的联系；序列模式挖掘则可以发现用户在时间序列上频繁出现的操作模式。

### 3. 接口设计

三级审计数据采集主要包括各安全应用系统(强制安全访问控制子系统、区域边界安全子系统等)审计数据采集。

(1) 模块功能及组成

在部署时各应用系统配置采集接口，各安全应用系统生成审计数据后直接读取三级安全审计数据采集接口，通过该接口将数据写入三级安全审计服务库。主要功能模块如下所述。

① 审计数据采集策略配置：各应用系统中的采集代理应先读取来自服务器端的审计数据采集策略，判断是否将所有审计数据都发送至三级安全审计服务器；如无该策略，则按照系统默认的采集策略执行；该配置过程可由服务器端或代理端完成。

② 通信配置：三级安全审计代理需要对网络通信进行运行配置，主要是审计数据库IP地址、密码等的配置。

③ 服务运行管理：审计代理应保持稳定持续运行，根据需要在代理端设定管理员以进行服务重启、暂停或停止操作。

(2) 处理流程

三级审计代理工作时，判断当前应用系统(强制访问控制、区域边界安全等子系统)是否产生主体访问异常事件，生成相应的审计数据；根据采集策略将相应的安全审计数据发送至三级安全审计数据库。

(3) 主要类函数

完成三级安全审计代理功能主要的类及函数见表 3-1。

表 3-1 主要类及函数列表

| 类 | 函数名 | 功能 |
|---|---|---|
| CPolicyAdd | OnAdd | 将审计数据采集策略写入代理端配置文件 |
| | OnRead | 读取策略文件(选择来自服务器或代理配置) |
| CCommuConf | AddDBConf | 添加数据库连接配置 |
| CServManage | Pause | 数据采集服务暂停 |
| | Restart | 数据采集服务重启 |
| | Stop | 数据采集服务停止 |
| | Start | 数据采集服务开始 |

## 3.8 典型应用子系统的设计和实现

OA 办公系统实现工作计划管理、公文管理、车辆管理、新闻管理、个人事务、信息交流等训练管理办公业务的网络化、自动化、数字化，从而提高训练管理日常办公效率和质量。

### 3.8.1 系统设计

OA 办公系统如图 3-13 所示，主要包括：工作计划、公文管理、车辆管理、个人事务、电子邮件、信息交流和办公平台。每个功能模块及其下的子模块均可通过用户权限进行灵活配置。在子模块中的具体操作权限也可通过角色进行严格定义。

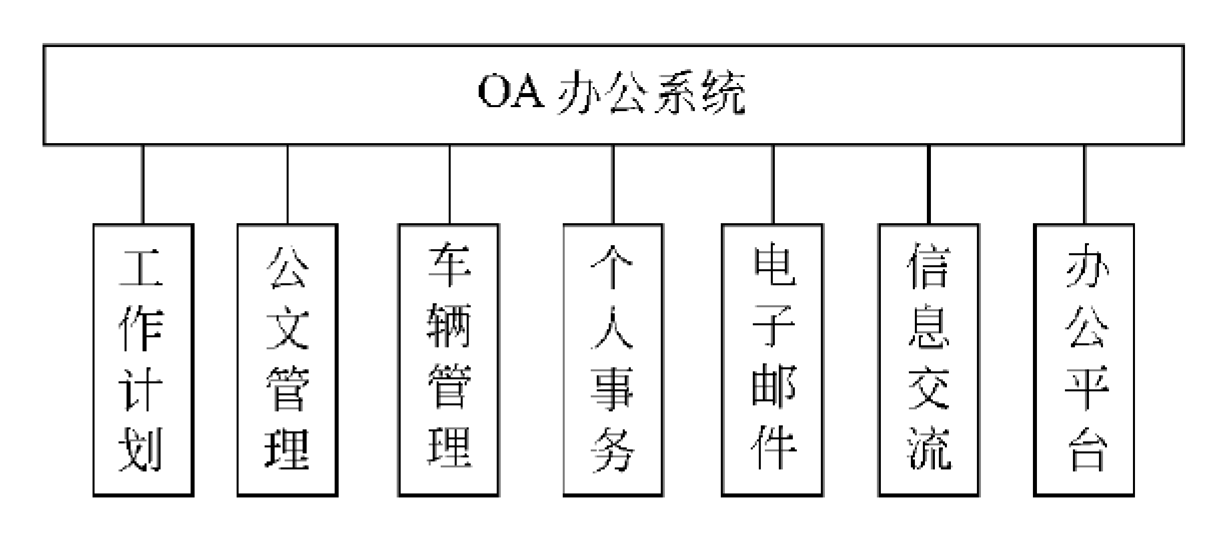



图 3-13 系统总体模块

### 1. 工作计划

工作计划模块实现训练部及各处室每周、每月工作计划的制定、呈报和审查等功能。工作计划管理模块包括处周工作计划、处月工作要点、查收周工作计划、查收处月工作要点、部周工作计划和部教学活动一览表六个子模块。

(1) 处周工作计划

① 编写处周工作计划：完成本周工作完成情况和下周工作计划的录入功能。

② 生成 Word 文档：将录入的本周工作完成情况和下周工作计划的内容自动转换为 Word 格式。

③ 呈报处周工作计划：将本周工作完成情况和下周工作计划呈报给训练部。

(2) 处月工作要点

① 上传/下载处月工作要点：完成处月工作要点上传或下载的功能。

② 呈报处月工作要点：完成处月工作要点向部里呈报的功能。

(3) 查收周工作计划

为部里提供查看、接收和审批各处室周工作计划的功能。

(4) 查收月工作要点

为部里提供查看、接收和审批各处室的月工作要点。

(5) 部周工作计划

① 编写部周工作计划：完成本周工作完成情况和下周工作计划的录入功能。

② 生成 Word 文档：将录入的本周工作完成情况和下周工作计划的内容自动转换为 Word 格式。

(6) 部教学活动一览表

查看各处室一周的教学活动情况，并能生成部教学活动一览表。

### 2. 公文管理

公文管理模块实现呈批件、通知的录入、Word 自动生成、报表打印、文档上传/下载等功能，公文管理模块包括呈批件管理、通知管理和文档管理三个子模块。

### 3. 车辆管理

车辆管理模块主要实现车辆基本信息的添加、修改和删除，使用车辆申请及对车辆申请的审批，当前车辆状态查看功能等。车辆管理模块包括车辆信息设置、出车申请和车辆管理三个子模块。

### 4. 个人事务

个人事务主要是为提高领导和机关行政人员办公效率提供的辅助手段，包括日程安排、通讯录、发布信息、信息订阅、网址收藏和个性化设置七个子模块。

### 5. 电子邮件

为用户之间发送和接收信息提供一种方便的、快捷的手段。电子邮件模块包括我的邮箱、写邮件、收件箱、发件箱、草稿箱、垃圾箱、地址簿和个人设置八个子模块。

### 6. 信息交流

信息交流模块为用户提供即时通信、发布信息、提出看法、聊天，获得帮助、讨论问题及为别人提供信息。信息交流模块包括内部论坛和即时通信两个子模块。

## 3.8.2 系统实现

### 1. 客体的标识与绑定

GB 17859—1999 规范了三级计算机信息系统应具备的安全和保证功能，而安全操作系统作为信息系统安全的核心，是安全应用平台的关键支撑部件，因此其所具有的安全功能和保证功能直接影响着应用系统的安全性，直接决定了信息系统的安全强度。显然，作为三级 Windows 操作系统，它也必须满足 GB 17859—1999 规定的安全功能要求和保证要求。

三级 Windows 操作系统需对系统中的客体(进程、文件等)进行全程的标记，确保主客体在整个生命周期中其标记的信息都是准确完整一致的。同时，标记应与内容绑定，保持完整一致，同时保证信息不能被篡改。

### 2. 强制访问控制关键技术

当对客体的实体加标记后，标记应由 TCB 管理和识别验证。如何结合 TCB 管理进行标记的识别与验证，是强制访问控制裁决模块应解决的关键问题。其主要包括以下四点。

① 提出应用封装技术，实现应用强制访问控制与应用流程的结合。

② 以 Windows 和 Linux 为主要操作系统平台进行安全增强，提高强制访问控制的适应性。

③ 与自主访问控制相结合，在保证原二级功能的基础上，进行三级安全增强。

④ 提出应用级强制访问控制和边界强制访问控制技术，使强制访问控制在 TCB 上向网络、计算环境和边界防护上的有效扩展。

### 3. 标记的安全管理

(1) 采用标记的安全管理技术，实现主体与客体的统一安全管理

客体的安全标记支持客体实体与标记的绑定，支持客体在网络上的传输。如何将客体进行安全管理，支持众多网络用户的安全标记管理，是基于标记的强制访问控制应解决的关键问题。

本系统中建立了安全管理中心，将主体、客体及其安全标记进行统一的安全管理，制定安全策略，使强制访问控制更易于实施。

(2) 提出基于标记的安全审计，明确用户的操作行为及相应安全机制作出的决策结果

一方面，在安全管理中心中增加安全审计模块，依据安全管理中心制定的审计策略，记录平台上用户的相应操作行为，尤其是用户违背系统安全策略的行为。审计模块和系统中的其他安全功能子模块(如标记子模块、访问控制子模块或身份鉴别子模块等)进行

通信，能够明确用户的操作行为及相应安全机制作出的决策结果。

另一方面，建立三级审计监控中心，与安全 VPN 系统、三级授权与访问控制系统相结合，记录应用系统和网络的安全日志，为三级平台的事后审计追踪提供决策依据。

### 4. 两种身份认证方式

系统中的用户首先要到认证中心进行身份注册，由认证中心进行用户的统一管理，保证用户身份的真实性。认证中心支持口令和 USB-KEY 两种身份认证方式，普通用户使用口令认证方式，进行重要操作的领导和管理员使用 USB-KEY 强认证方式，只有通过认证的用户才能登录应用系统，防止身份假冒威胁。

### 5. 用户安全标识

按照 GB 17859—1999 的要求，为用户分配安全标识。

用户安全标识由级别和范畴集两部分组成。用户的级别为个人所能处理信息的最高级别，范畴集为用户的部门和岗位。

### 6. 资源安全标识

由授权管理系统为应用系统的功能菜单和操作分配安全标识，安全标识由级别和范畴集两部分组成。级别为资源的重要程度，范畴为资源可被使用的范围。训练管理信息系统的主要资源安全标识如下所述。

(1) 工作计划管理

工作计划管理模块的安全级见表 3-2。

表 3-2　工作计划管理模块安全级列表

| 资　源 | 级别 | 范畴集 | 资　源 | 级别 | 范畴集 |
|---|---|---|---|---|---|
| 工作计划管理 | 2 | | 部周工作计划 | 3 | 部 |
| 处周工作计划 | 2 | 处 | 部月工作要点 | 3 | 部 |
| 处月工作要点 | 2 | 处 | 查收部周工作计划 | 3 | 部、查收 |
| 查收处周工作计划 | 2 | 处、查收 | 查收部月工作要点 | 3 | 部、查收 |
| 查收处月工作要点 | 2 | 处、查收 | | | |

(2) 公文管理模块

公文管理模块的安全级见表 3-3。

表 3-3　公文管理模块的安全级列表

| 资　源 | 级别 | 范畴集 | 资　源 | 级别 | 范畴集 |
|---|---|---|---|---|---|
| 公文管理 | 2 | | 通知管理 | 2 | |
| 呈批件管理 | 2 | | 文档管理 | 2 | |

(3) 车辆管理模块

车辆管理模块的安全级见表 3-4。

表 3-4 车辆管理模块的安全级列表

| 资 源 | 级别 | 范畴集 | 资 源 | 级别 | 范畴集 |
|---|---|---|---|---|---|
| 车辆管理 | 1 | | 出车申请 | 1 | |
| 车辆信息设置 | 1 | 军务 | 派车管理 | 2 | 军务,主任 |

(4) 个人事务模块

个人事务模块的安全级见表 3-5。

表 3-5 个人事务模块的安全级列表

| 资 源 | 级别 | 范畴集 | 资 源 | 级别 | 范畴集 |
|---|---|---|---|---|---|
| 个人事务 | 1 | | 信息订阅 | 1 | |
| 日程安排 | 1 | | 网址收藏 | 1 | |
| 通讯录 | 1 | | 个性化设置 | 1 | |
| 发布信息 | 1 | | | | |

(5) 电子邮件模块

电子邮件模块的安全级见表 3-6。

表 3-6 电子邮件模块的安全级列表

| 资 源 | 级别 | 范畴集 | 资 源 | 级别 | 范畴集 |
|---|---|---|---|---|---|
| 电子邮件 | 1 | | 草稿箱 | 1 | |
| 我的邮箱 | 1 | | 垃圾箱 | 1 | |
| 写邮件 | 1 | | 地址簿 | 1 | |
| 收件箱 | 1 | | 个人设置 | 1 | |
| 发件箱 | 1 | | | | |

(6) 信息交流模块

模块为用户提供即时通信、发布信息、提出看法、聊天、获得帮助、讨论问题及为别人提供信息。信息交流模块包括两个子模块。信息交流模块的安全级见表 3-7。

表 3-7 信息交流模块的安全级列表

| 资 源 | 级别 | 范畴集 |
|---|---|---|
| 信息交流 | 1 | |
| 即时通信 | 1 | |
| 内部论坛 | 1 | |

## 7. 强制访问控制

应用系统在收到用户访问请求时,根据用户的安全标识与所请求的资源标识决定是

否允许访问。若用户的安全级支配资源的安全级则允许访问。如军务办的普通用户，其安全级为 1，范畴集为“军务”，根据强制访问控制规则，可以访问车辆管理模块以及车辆信息设置二级资源，但是由于范畴集中没有“科长”的范畴，则无法访问“派车管理”菜单，不能进行派车。军务办科长的范畴集中包含“军务”和“科长”，因此可以访问“派车管理”进行派车审批。

#### 8. 应用授权与自主访问控制

按照用户在系统中的权限，对应用系统的功能菜单和操作进行授权，形成访问控制列表。用户在访问应用系统时根据应用访问控制列表决定用户的访问行为是否能够进行。

#### 9. 安全传输

使用 VPN 系统对网络传输数据进行保护，通过 IPSec 协议和密码算法对传输数据实现机密性和完整性保护。

#### 10. 安全存储

使用安全公文包实现个人终端上的存储保护，通过安全中间件、密码算法和 USB 密码钥匙实现用户透明的数据机密性和完整性保护。

#### 11. 安全审计

按照三级信息系统的要求训练管理信息系统，除了进行通常的应用审计以外，还要求记录与强制访问控制相关的用户访问行为和结果，至少包括用户名、用户安全级、客体名、客体安全级、访问结果和访问时间等，若访问被拒绝还要记录拒绝原因。并且要将强制访问控制审计记录同步到三级审计中心。

## 3.9 示范环境功能使用操作演示

### 3.9.1 安全计算环境子系统

安全策略的制定过程包括三个阶段。

① 初始设置阶段：首先进行安全设计，即系统管理员收集全系统的用户身份和平台资源信息，由授权机构依据该信息对主客体的安全标记以及访问控制规则进行设计，制定符合系统安全的策略配置，安全管理员将上述信息导入到管理中心；然后构建系统 TCB，即安装终端节点安全操作系统、设置区域边界和网络传输设备，确保系统运行时能够从安全管理中心下载策略，保证 TCB 的正常工作；最后安装应用系统，即系统管理员根据应用需求安装应用系统。

② 系统测试阶段：初始设置完成后，系统从管理中心下载策略，进入试运行阶段。但由于预先制定的策略可能不完善，或者存在限制过严的情况，系统需要将运行情况上报管理中心，方便安全管理员参考，从而对安全策略实施调整，直至系统和应用服务正常运行。

③ 运行服务阶段：应用服务开始运行，TCB 依据安全策略对主体行为进行访问控

制，安全管理员根据需要对策略进行维护和更新。

### 1. 初始设置阶段

(1) 管理员账号管理

账号管理员依据主体标记中的管理员类型信息添加安管平台的安全管理员、系统管理员、安全审计员账号。打开“三级安全应用平台安全管理中心”页面，选择“账号管理”命令，在弹出的页面的文本输入管理员名和密码(默认为“superadmin”，“admin”)。

(2) 发行用户硬件令牌(令牌发行操作)

发 KEY 操作只能在安全管理平台所在的机器上进行，首先将要发的 KEY 插在安全管理中心上，然后打开安全管理中心，使用系统管理员登录安全管理中心，选择操作栏中的“用户管理”中的“下发令牌”命令，发行 KEY，如图 3-14 所示。

图 3-14 “下发令牌”操作界面

写入 KEY 需要一定时间，当发 KEY 成功后，会弹出“发 KEY 成功”对话框，单击“确定”按钮，即可完成发 KEY 操作。

(3) 系统管理员进行初始化工作

使用平台注册工具获取平台硬件标识和基本信息，上报到系统管理平台。使用可执行程序采集工具生成可执行程序列表，上报到管理平台。系统管理员登录安管平台，依据策略进行如下管理：

① 系统文件列表管理；

② 可执行代码预期值管理；

③ 受限网络 IP 管理。

(4) 安全管理员制定策略

安全管理员登录安管平台，依据系统管理员提供的配置信息以及十个策略制定参考表中的内容，实施标记和授权。其内容包括：

① 范畴关系管理；
② 主体标记列表管理；
③ 客体标记列表管理；
④ 入自主访问控制策略管理；
⑤ 级别调整策略管理；
⑥ 系统文件实施授权；
⑦ 将可执行程序进行授权给指定平台和指定用户；
⑧ 对非 IPSec 控制平台进行授权；
⑨ 终端授权用户管理。

### 2. 系统测试阶段

① 节点、边界和应用防护墙启动。记录可执行程序预期值和文件访问操作，形成策略申请包上报安全管理中心。

② 系统管理员可执行代码预期值管理。

③ 安全管理员可执行代码预期值授权。安全管理员将可执行程序列表中的合法程序执行权限授予相应的用户。

④ 自主访问控制策略。将文件访问操作权限授予相应用户，加入自主访问控制列表，单击在左边操作栏“策略管理”下的“查看策略申请”命令，进入策略申请管理主界面。

⑤ 安全管理员将平台策略控制状态设置为“运行服务”后，系统调试阶段完成。

### 3. 运行服务阶段

① 节点启动后，下载平台已经有用户相关的策略，所有安全控制模块开启，开始正常运行，并进行实时审计。

② 安全管理员策略调整。安全管理员根据系统运行状态以及授权机构的策略修改信息，更新策略并实施策略更新。

③ 审计管理。安全管理员为每个审计类型设定事件级别，分为高风险、中风险和低风险三种，为每一个子类型制定审计时间和成败审计。可以进行审计策略的修改和查询。

## 3.9.2 安全区域边界子系统

### 1. 主要操作界面

管理用户登录仅采用用户名和口令方式的认证。用户名：clf，密码：999999。当管理用户登录后，出现首页，如图 3-15 和图 3-16 所示。

网关设备信息：设备名称、设备序列号、软件版本号、运行时间、系统时间；

接口信息：接口名、IP 地址、MAC 地址、连接状态、工作状态、接收速率与发送速率；

系统资源：CPU 利用率、内存占用率；

平台信息：集中管理平台、审计管理中心、密钥管理中心；

注明：“更多”关联网络管理的“接口”。

欢迎使用区域边界防护管理系统

用户名： 密 码：

图 3-15 区域边界防护管理系统用户登录界面

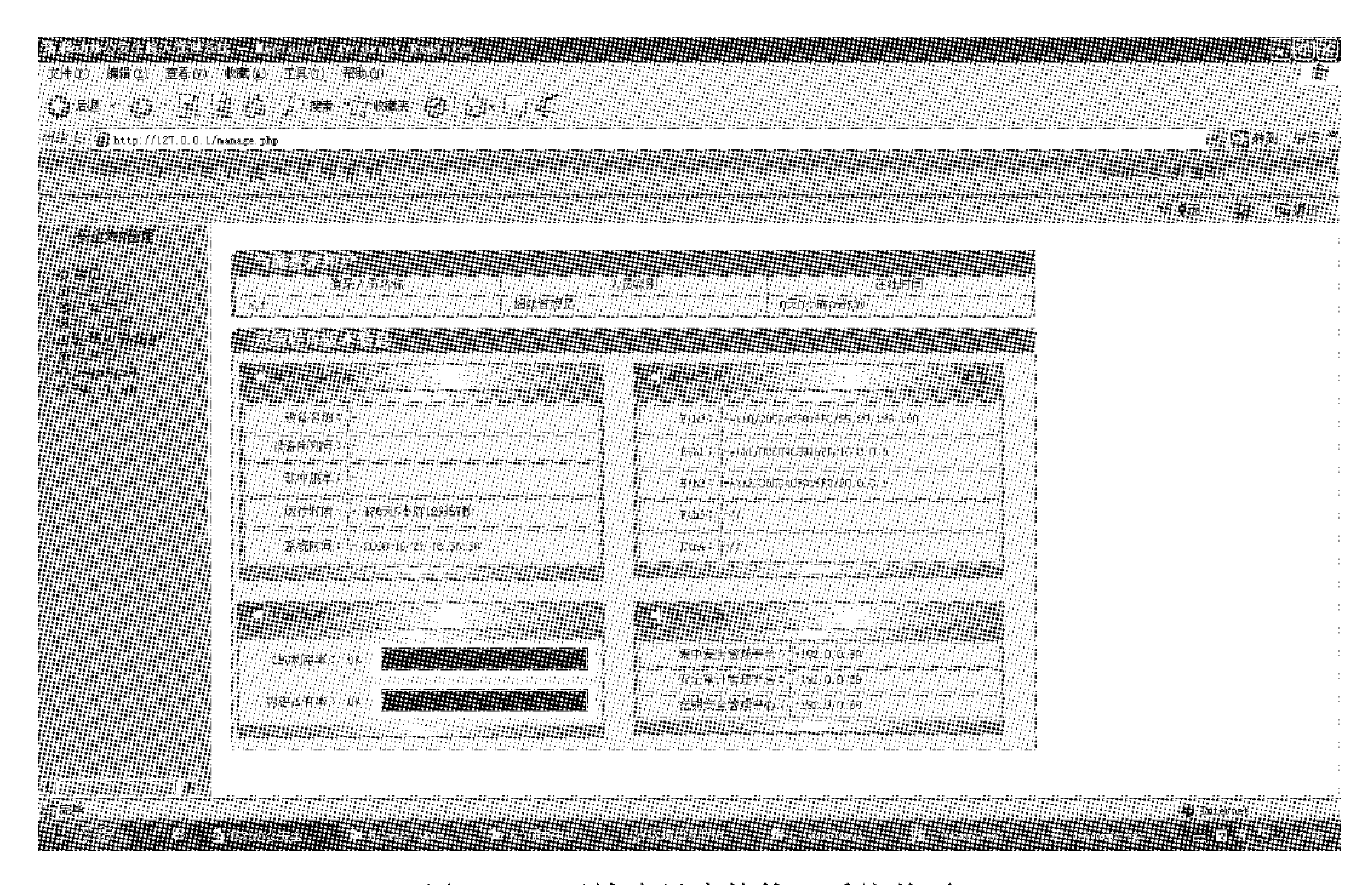


图 3-16 区域边界防护管理系统首页

## 2. 网络配置

网络配置下拉菜单的内容有：接口、安全区域、路由信息以及网络维护，如图 3-17 所示。

## 3. 标记管理

标记管理是实现三级平台下 VPN 系统的重要基础。其功能包括：安全级管理、用户管理、地址对象管理和服务对象管理，如图 3-18 所示。

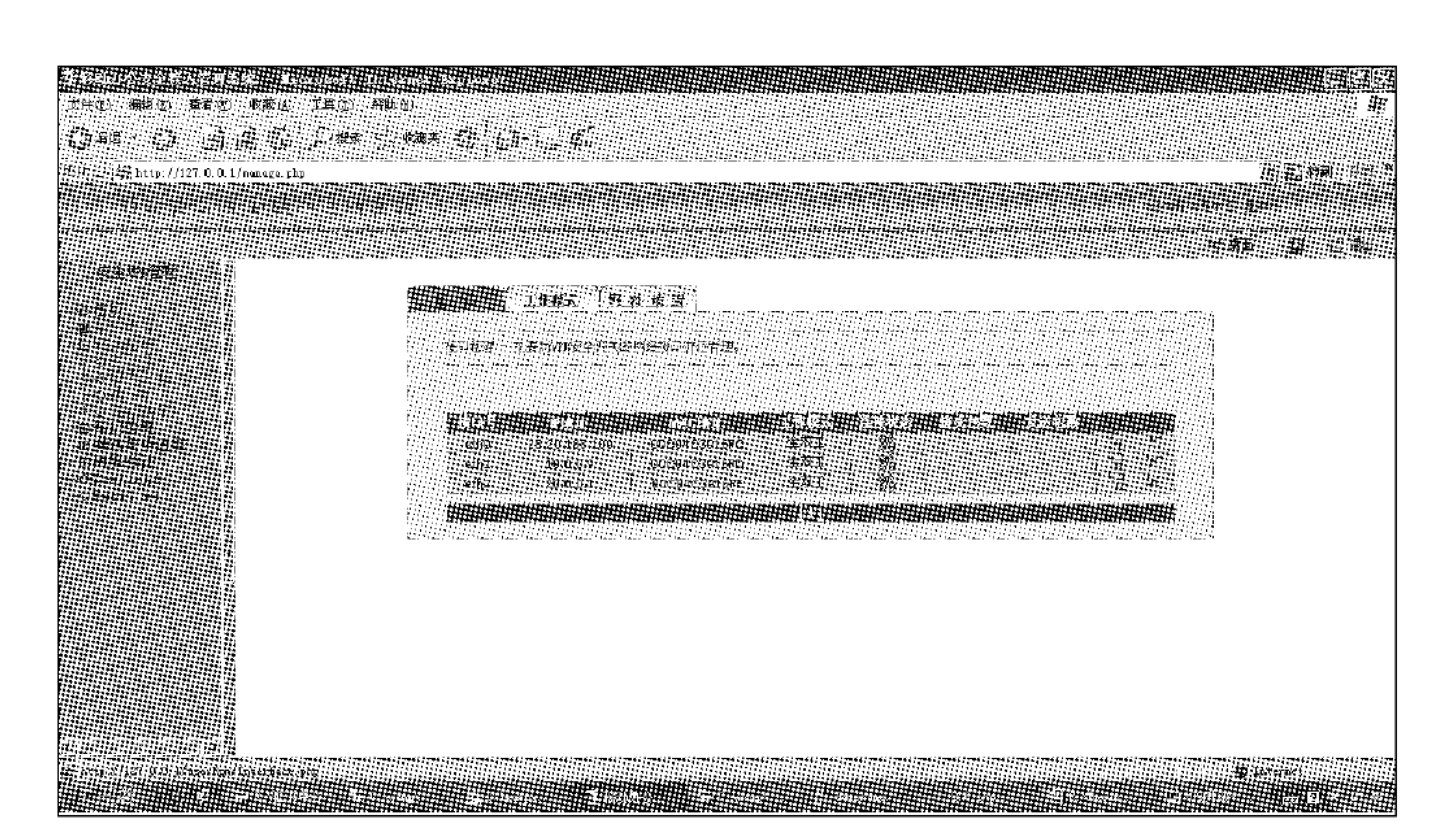


图 3-17　网络配置界面

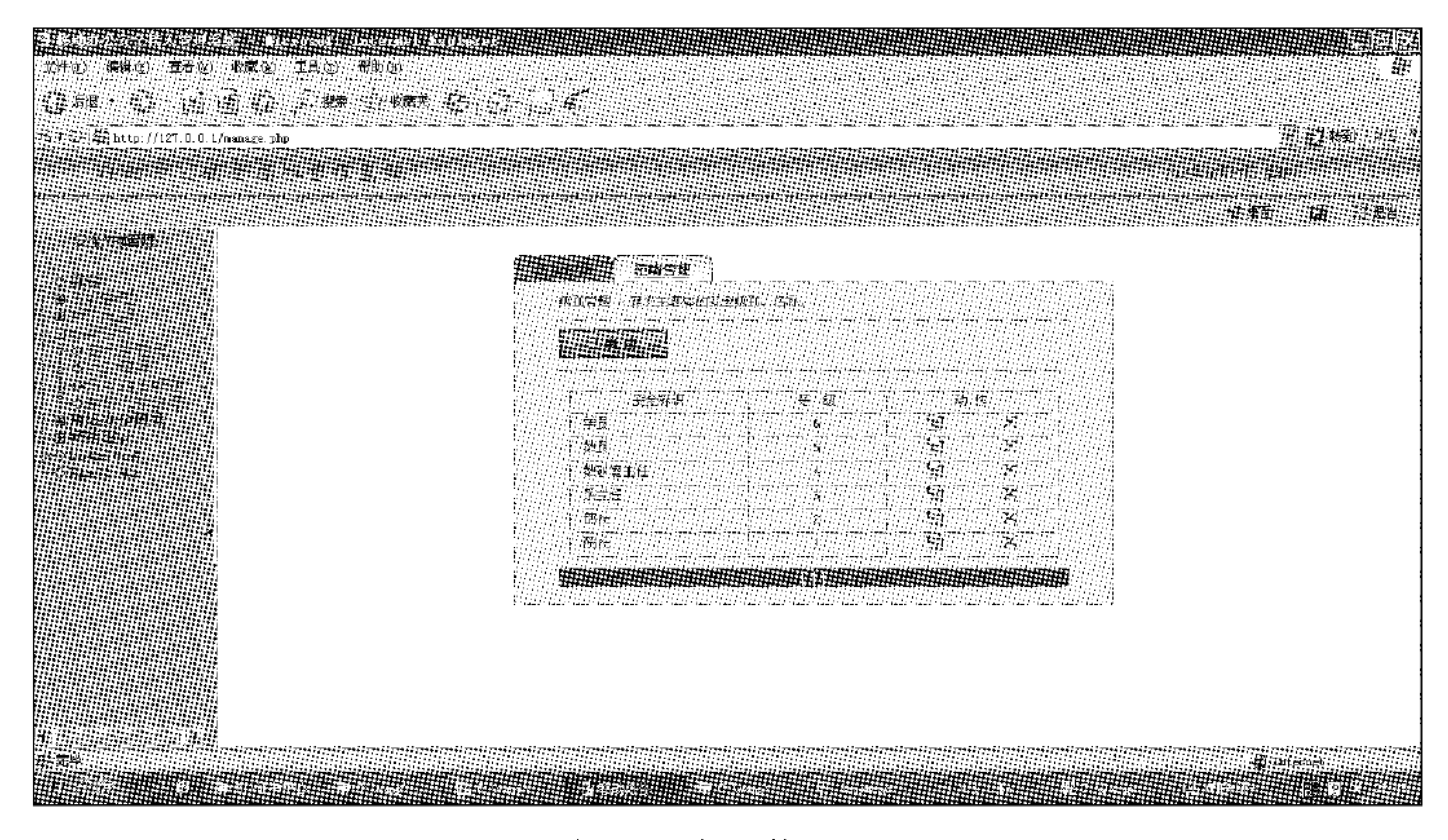


图 3-18　标记管理界面

### 4. 区域边界防护

区域边界防护主要包括防火墙包过滤策略管理与 NAT 策略管理，如图 3-19 所示。

### 5. 网络审计

网络审计管理，主要是基于用户的审计。考虑在静态隧道下，是否可以是基于对象的审计，只需要 Web 对这类审计会显示、查找数据库判断 IP 地址或者子网属于哪个对象并转换即可。主要包括刷新审计和审计的查询，如图 3-20 所示。

当选择某一个查询方式时，其他方式对应的信息框变成灰色，单击“查询”按钮(注意在输入查询条件时，要和提示的一致。如时间一定要是 yyyy-mm-dd，地址节点一定是：

***.***.***.***,并且必须既有源地址也要有目标地址)。删除审计信息,则在单击“删除”按钮后会完全删除数据库中的审计信息。

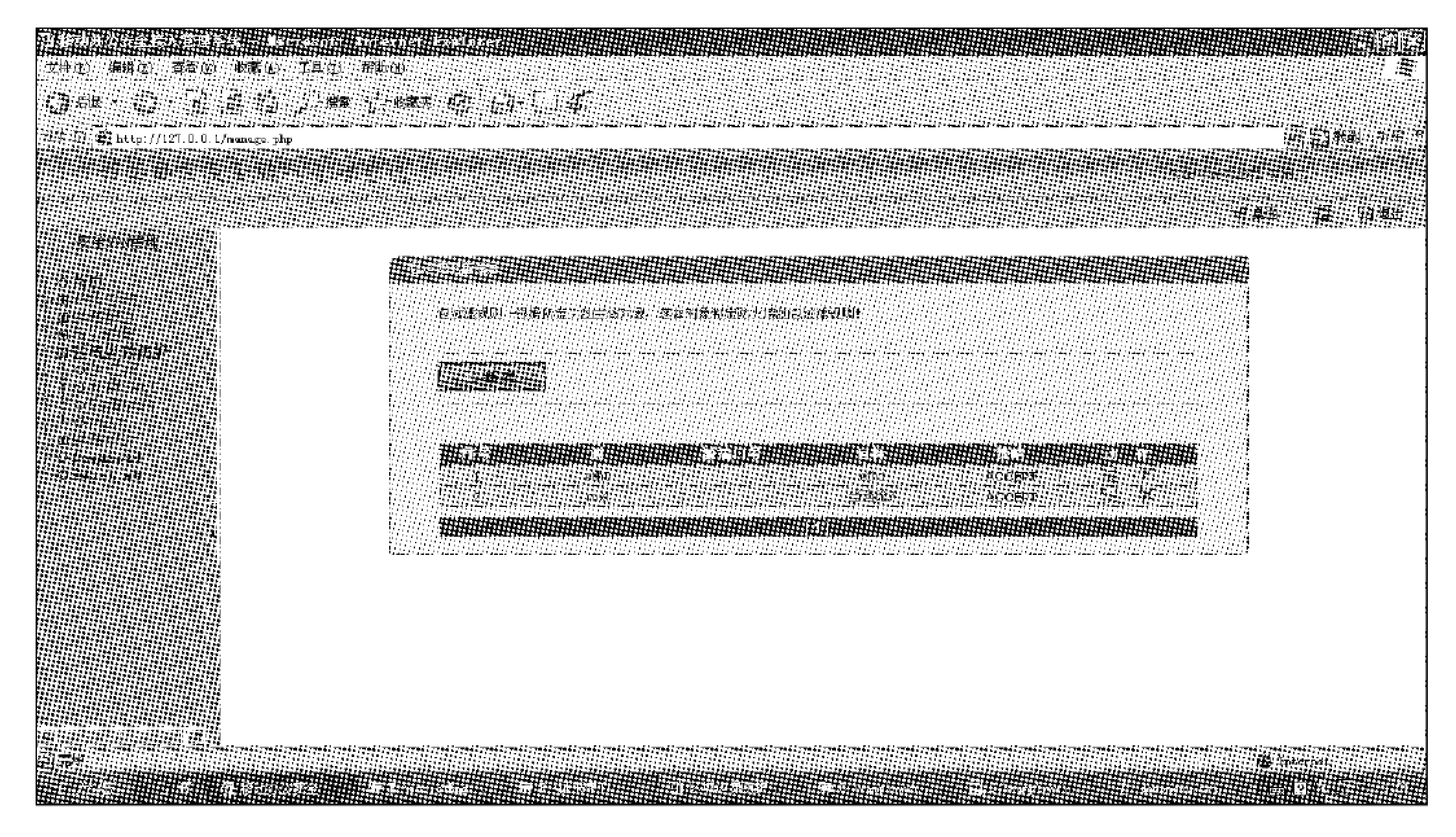


图 3-19 区域边界防护界面

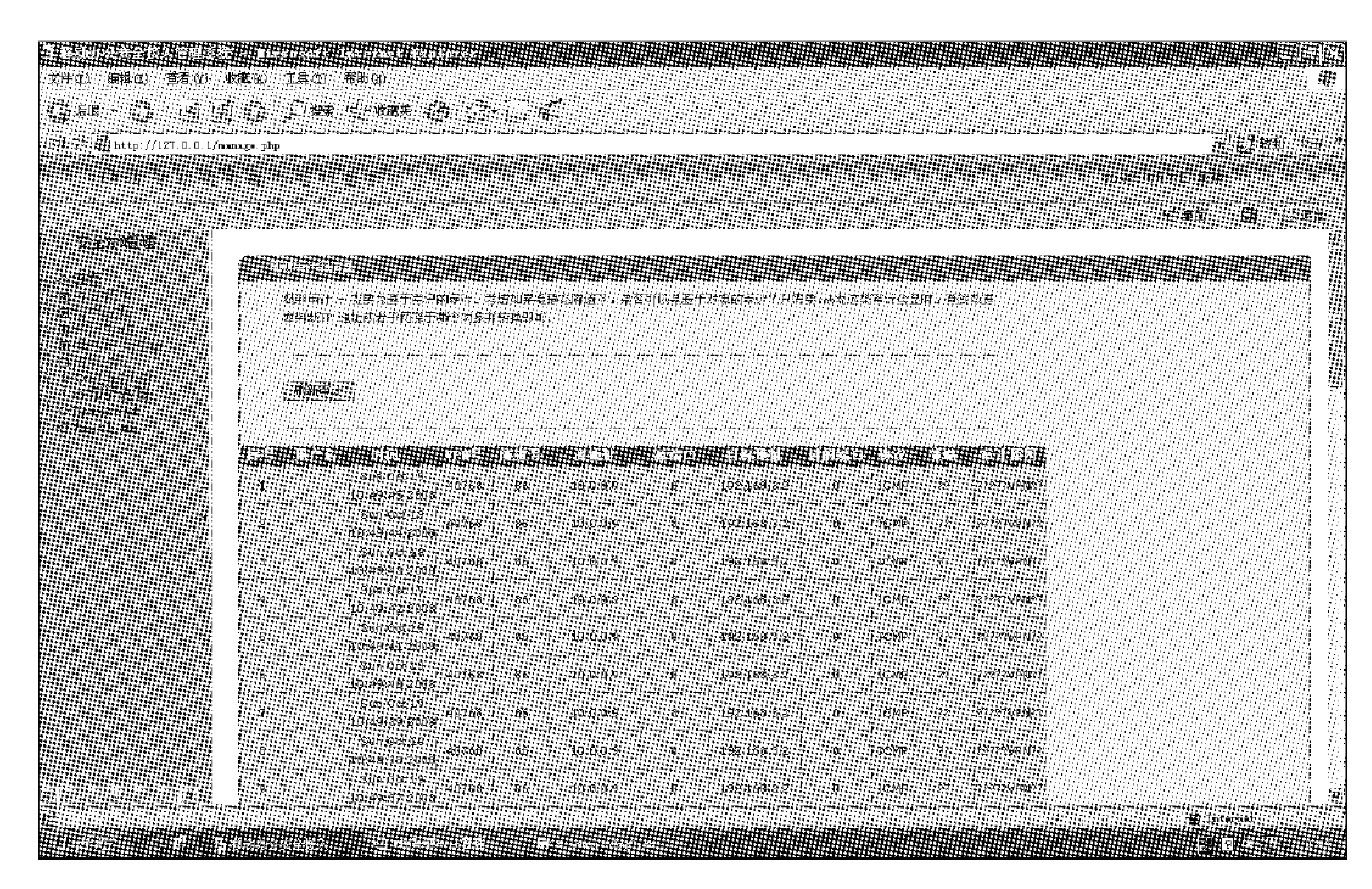


图 3-20 网络审计管理界面

## 3.9.3 安全通信网络子系统

### 1. 主要操作界面

管理用户登录仅采用用户名和口令方式的认证。用户名:clf,密码:999999,如

图 3-21 所示。

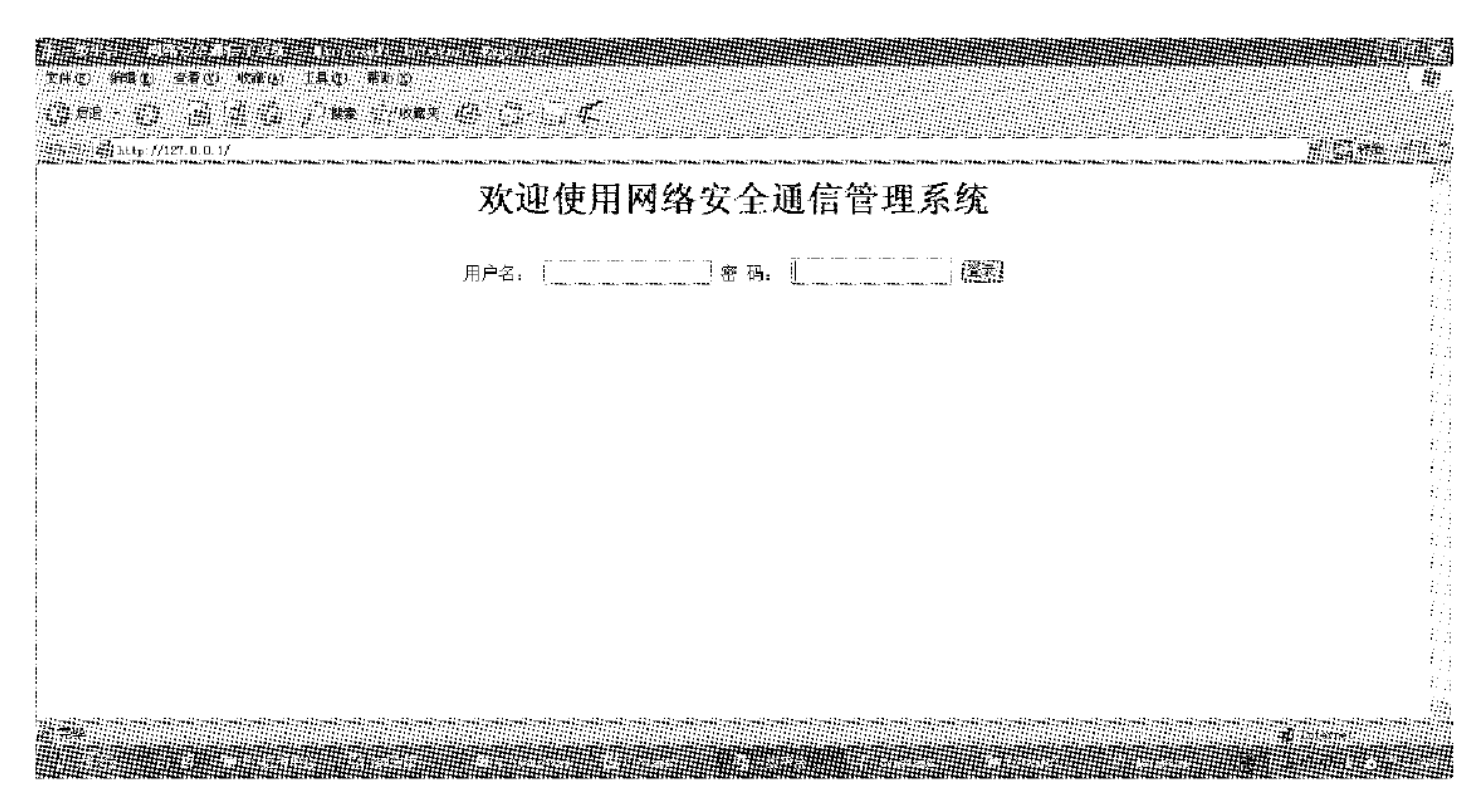



图 3-21　网络安全通信管理系统用户登录界面

当管理用户登录后，会出现首页，如图 3-22 所示。

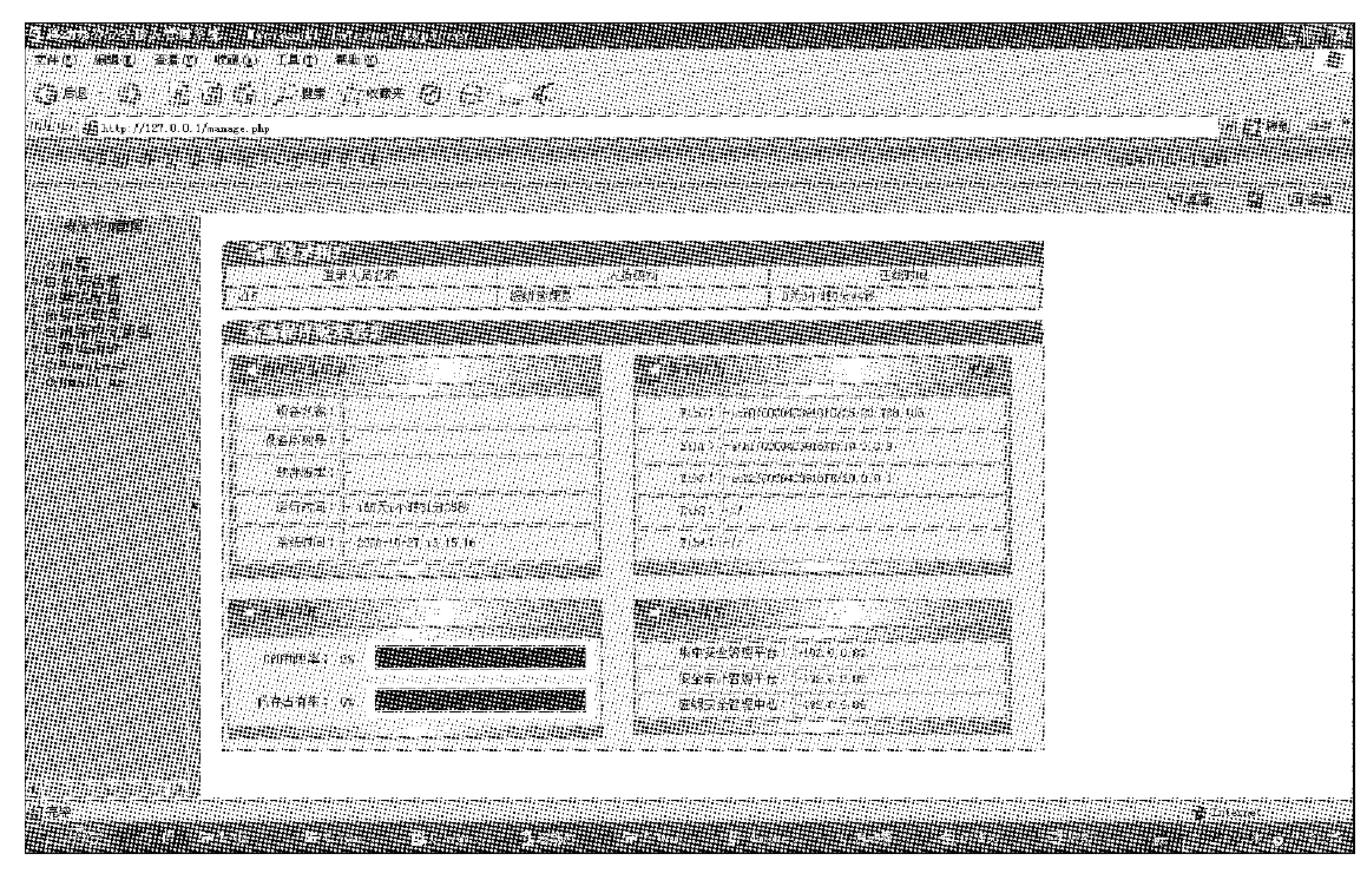


图 3-22　网络安全通信管理系统首页

## 2. 网络配置

网络配置，包括的下拉菜单内容有接口、安全区域、路由信息以及网络维护，如图 3-23 所示。



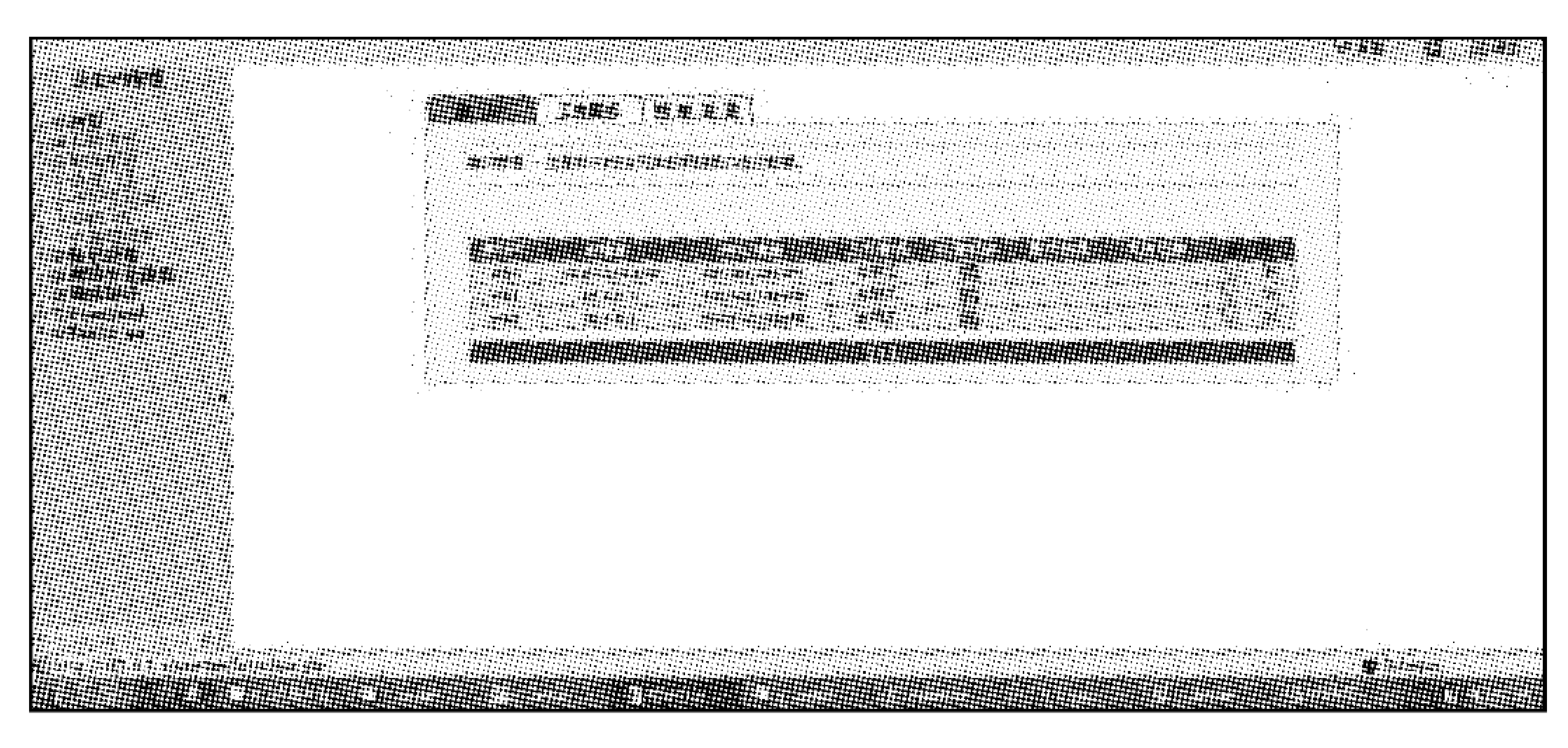


图 3-23 网络配置界面

### 3. 地址对象管理

地址对象管理包括地址节点与地址组的管理，主要是解决单个地址节点、子网节点和地址组等对象的管理，如图 3-24 所示。

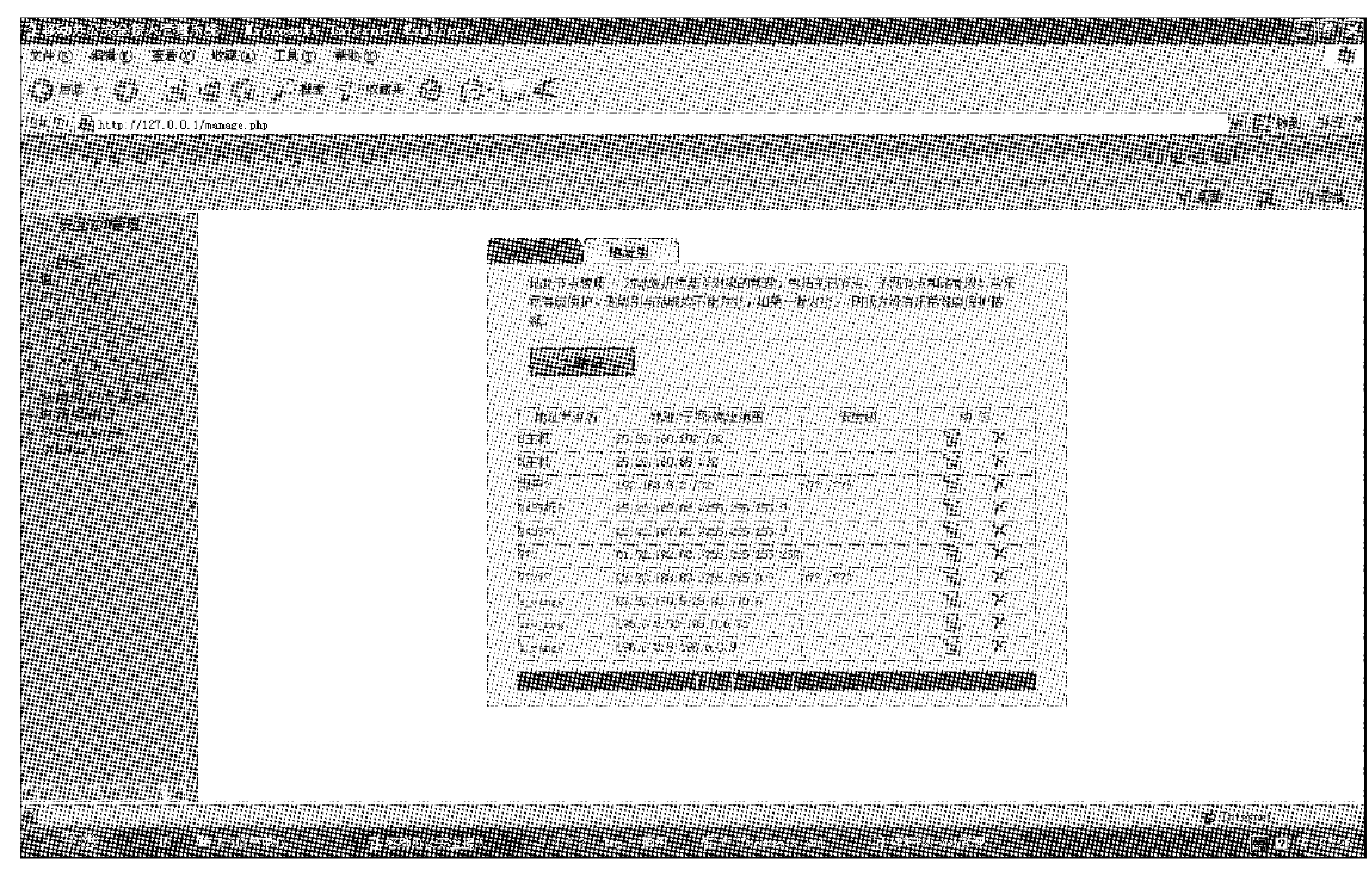


图 3-24 地址对象管理界面

单击动作栏中的“修改”或“添加”按钮，可以对现有的级别进行修改或删除，单击“修改”按钮弹出修改对话框，如图 3-25 所示。

自定义服务为管理根据具体情况定义的服务对象。例如，车购税系统 TCP：7777。主界面如图 3-26 所示。

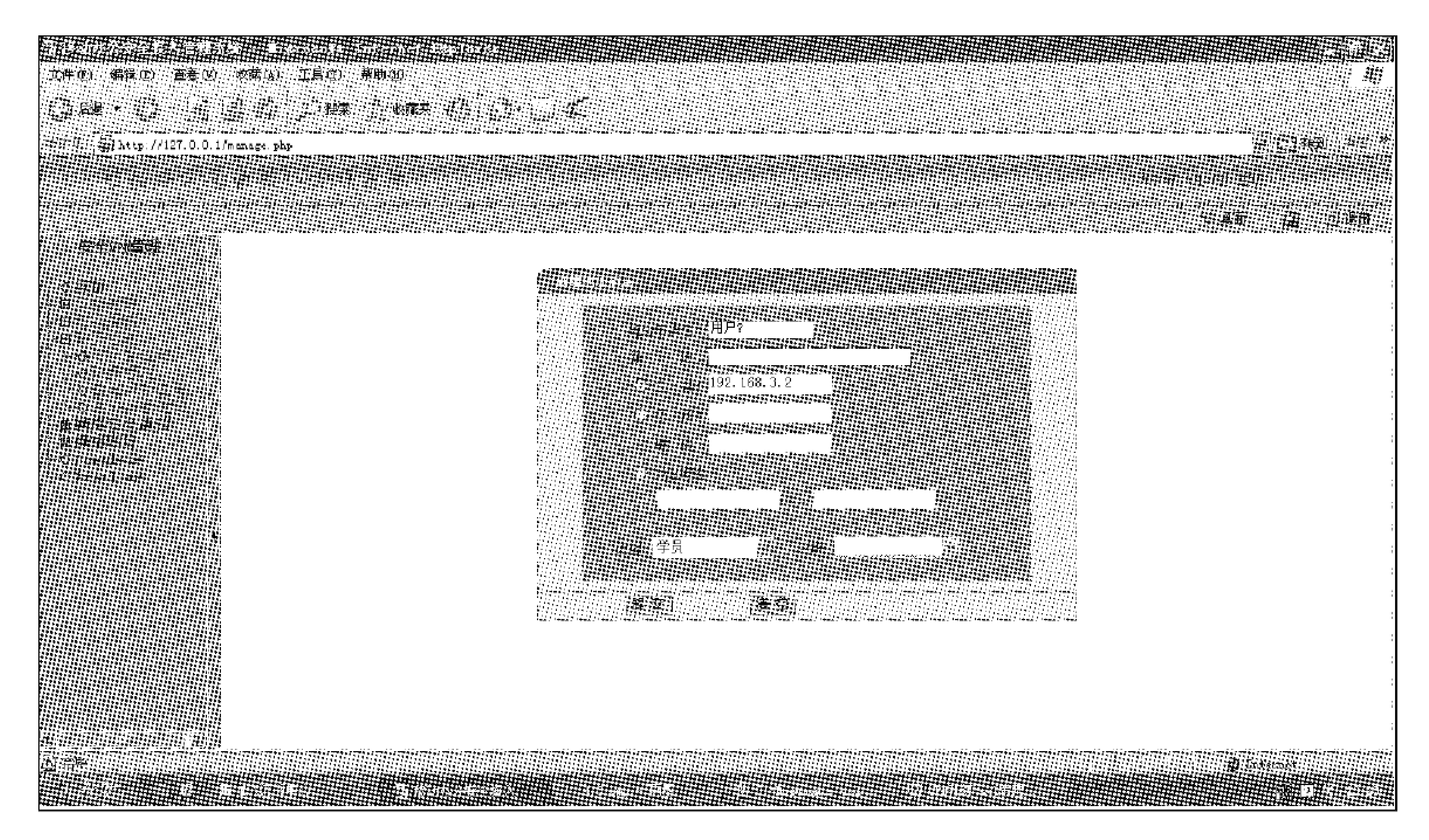


图 3-25　修改对话框

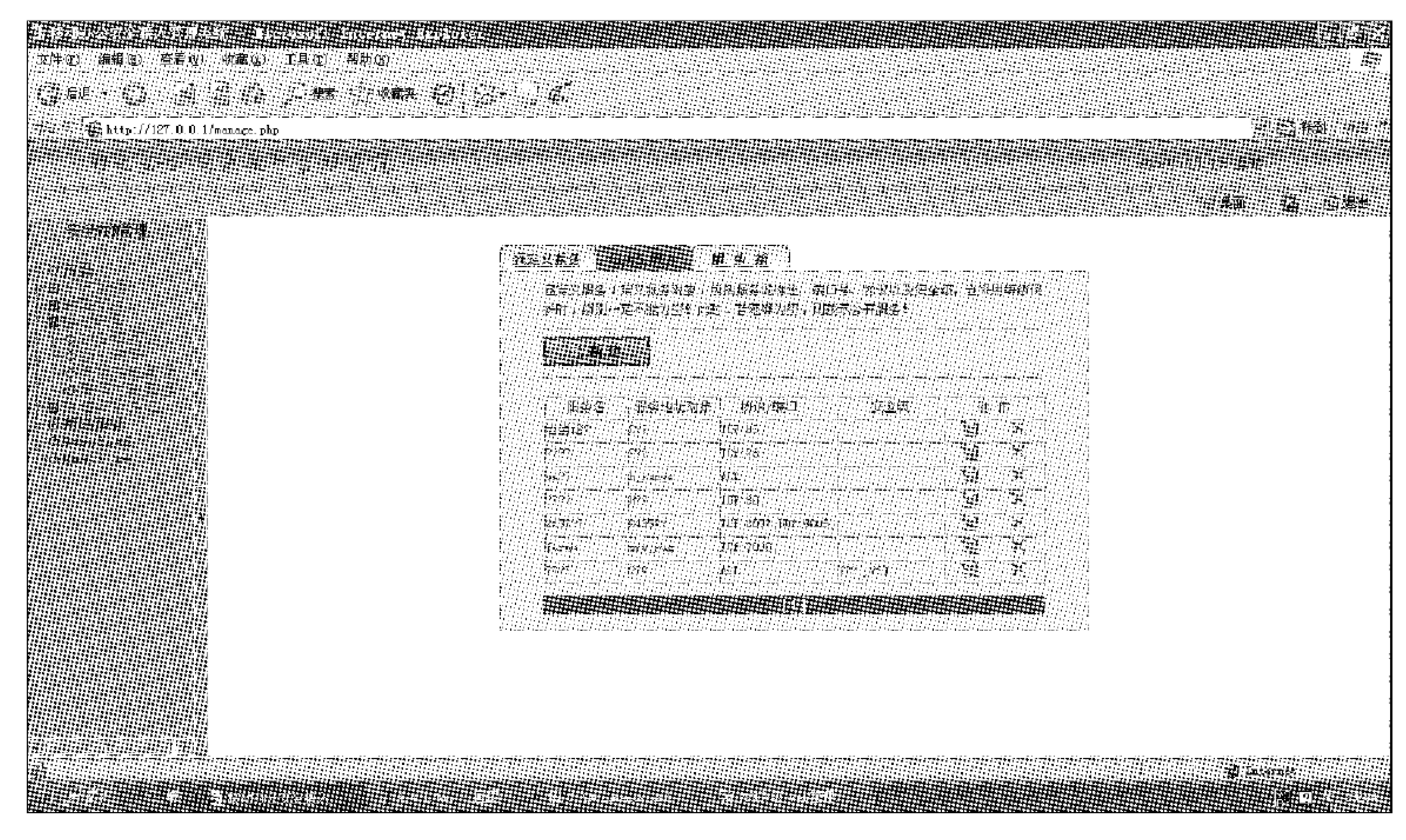


图 3-26　自定义服务主界面

### 4. 网络安全通信

安全隧道分为静态与动态安全隧道。静态隧道是针对 VPN 设备地址确定的情况，而动态隧道则是 VPN 设备地址不确定的情况。安全隧道配置列表显示界面如图 3-27 所示。

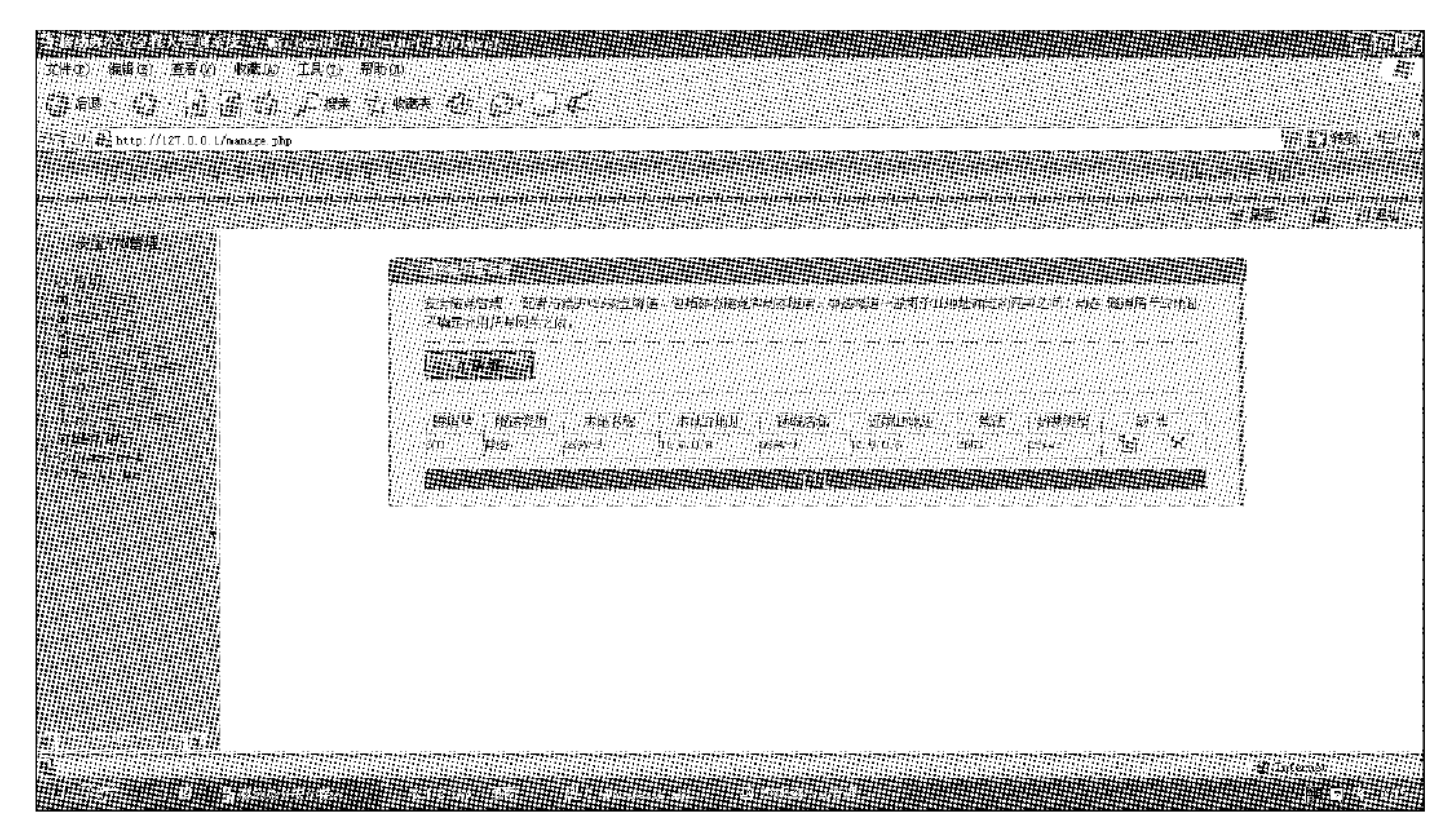


图 3-27　安全隧道配置列表显示界面

单击"修改"按钮，进入安全隧道配置界面，安全隧道配置包括安全隧道类型(动态、静态)、隧道号、封装类型(IPSec、NAT 穿越、UDP 封装)、本机设备名、本机设备 IP 地址、远端设备名、远端设备 IP 地址(静态)、算法号、密钥(静态)。

以主体、客体的形式定义策略。VPN 安全策略管理主界面如图 3-28 所示。

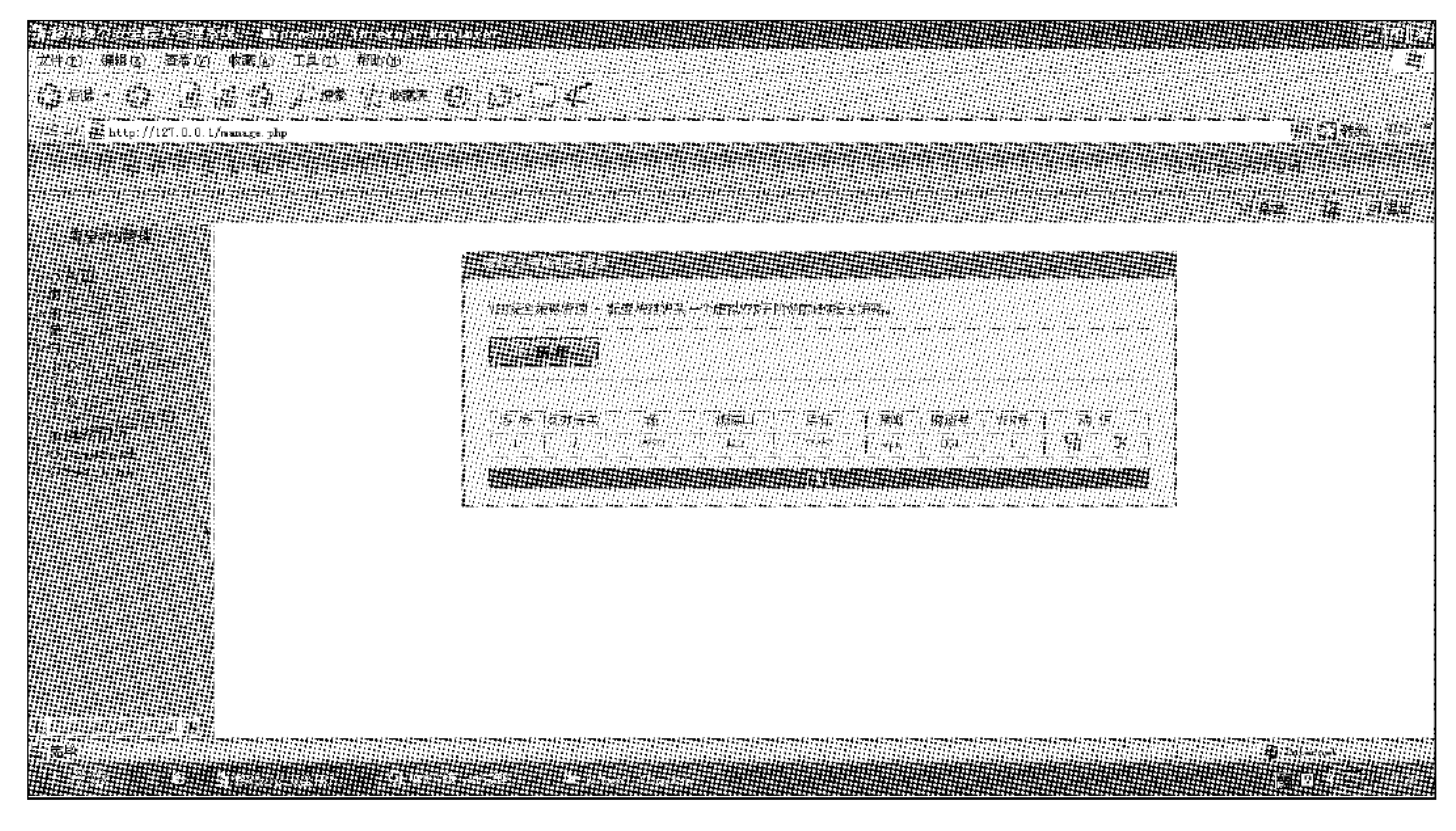


图 3-28　VPN 安全策略管理主界面

## 5. 网络审计

网络审计管理，主要是基于用户的审计。考虑在静态隧道下，是否可以是基于对象的审计，只需要 Web 对这类审计会显示，查找数据库判断 IP 地址或者子网属于哪个对象并转换即可。主要包括刷新审计和审计查询。

刷新审计：用户名/对象名、时间、VPN 号、隧道号、源地址、目标地址、协议、策略、审计原因。

审计查询：用户名/对象名、时间和地址(三种查询方式)。审计查询界面如图 3-29 所示。

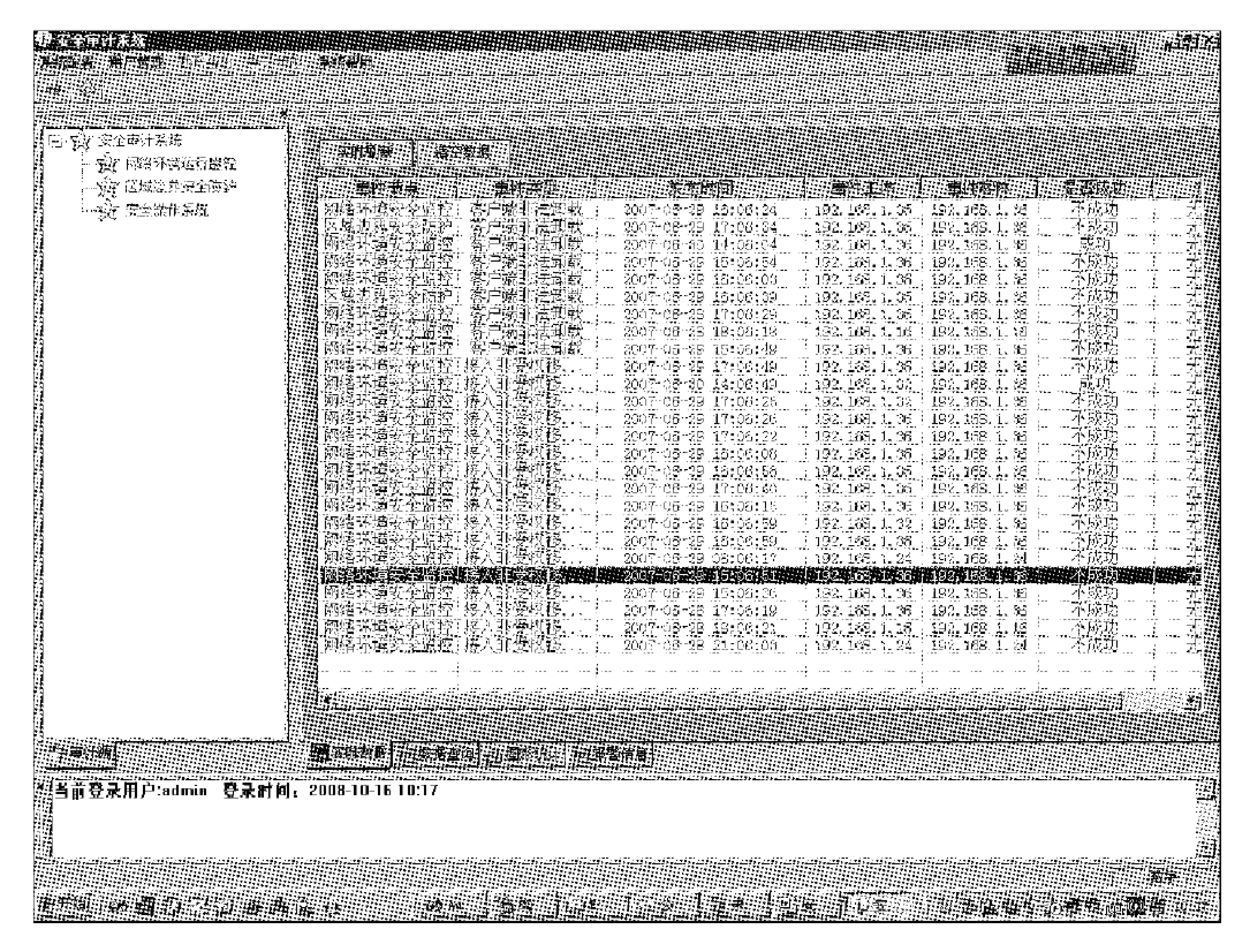



图 3-29 安全审计系统主界面

## 3.9.4 安全审计子系统

### 1. 系统主界面

系统主界面如图 3-29 所示。

系统主界面中，上方为菜单项，主要是系统级功能，如系统配置、用户管理等；左边为系统树形目录，显示已有的业务系统；右边为系统功能主界面；下边显示当前登录用户及登录时间。

### 2. 数据查询

在右边单击“数据查询”按钮，将显示数据查询主界面。它提供两种查询方式即模糊查询和组合查询，模糊查询只需要输入事件主体关键字部分内容即可，如图 3-30 所示。

### 3. 图形统计

图形统计以直观形式显示数据。统计方式分两类，一类为可选事件，即以事件发生时间为条件统计，一类为全部事件；图形类型为柱状、饼状两种；详细的统计条件为事件节点、类型、主体及事件是否成功四类，如图 3-31 所示。

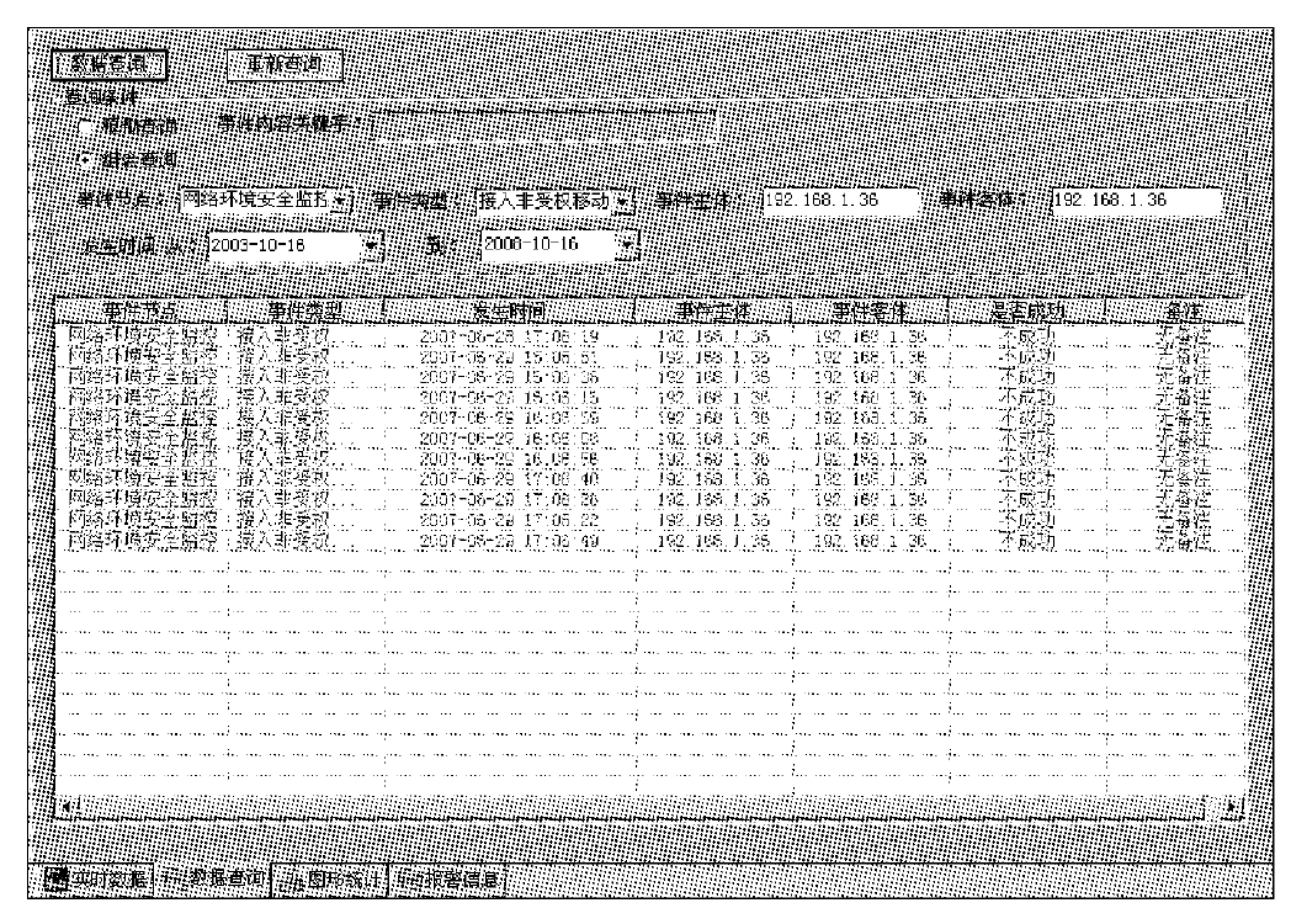


图 3-30 数据查询主界面

### 4. 异常报警

异常报警是对所有安全审计事件进行简单异常分析，主要是对各业务系统中用户异常操作进行判断、统计，提供异常信息。

异常分析是针对已选择节点、相应的事件类型及发生时间段，根据已定制的报警策略，对已有数据进行统计并报警。

异常分析报警策略需要事先定义。针对所有事件类型，用户可定义相应的异常报警信息及级别。“报警规则设置”界面如图 3-32 所示。

### 5. 用户管理

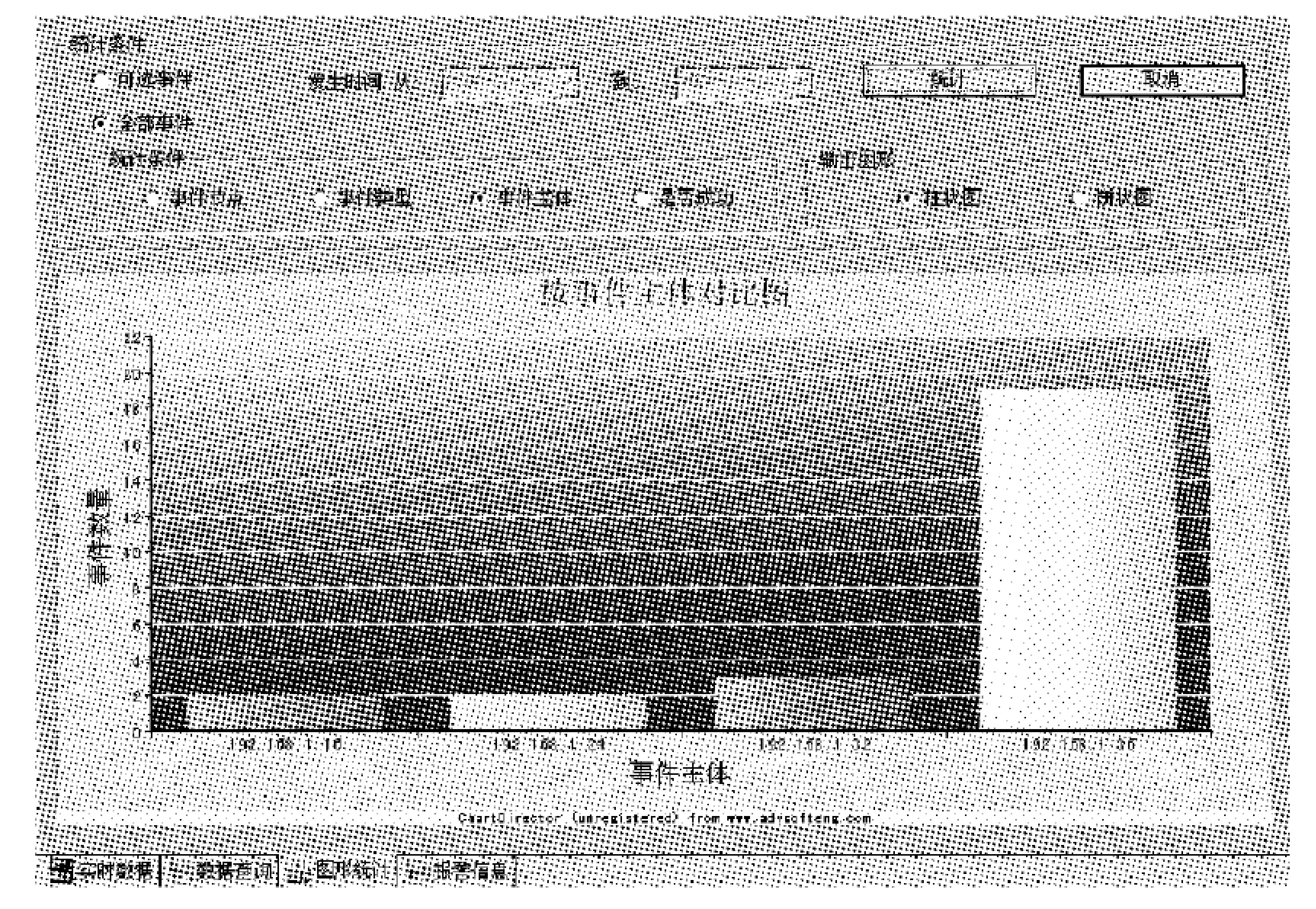
用户管理进行简单的身份鉴别，可建立两类用户：普通用户及管理员。普通用户主要进行数据查询等操作，管理员可查看报警信息及用户添加删除、数据删除等操作。

## 3.9.5 典型应用子系统

### 1. 工作计划

① 新建处周工作计划基本信息，并进一步填写本周完成情况的基本信息，如图 3-33 所示。

② 添加工作任务和教学活动条目。分别在本周完成情况和下周计划页面中添加工作任务和教学活动条目。单击“呈报”和“生成文档”按钮进行呈报和生成文档操作，如图 3-34 所示。



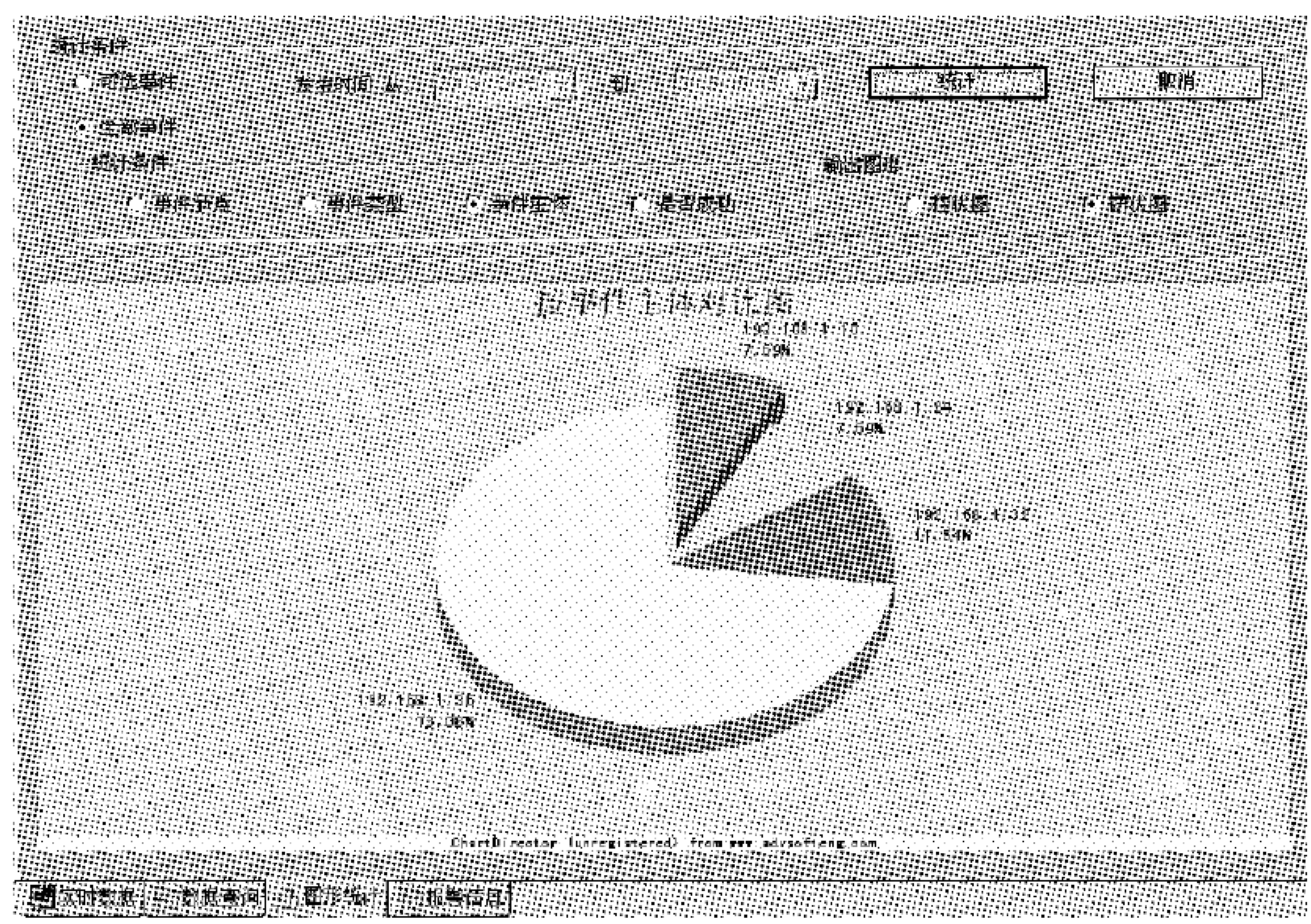


图 3-31　图形统计界面

图 3-32　报警规则设置界面

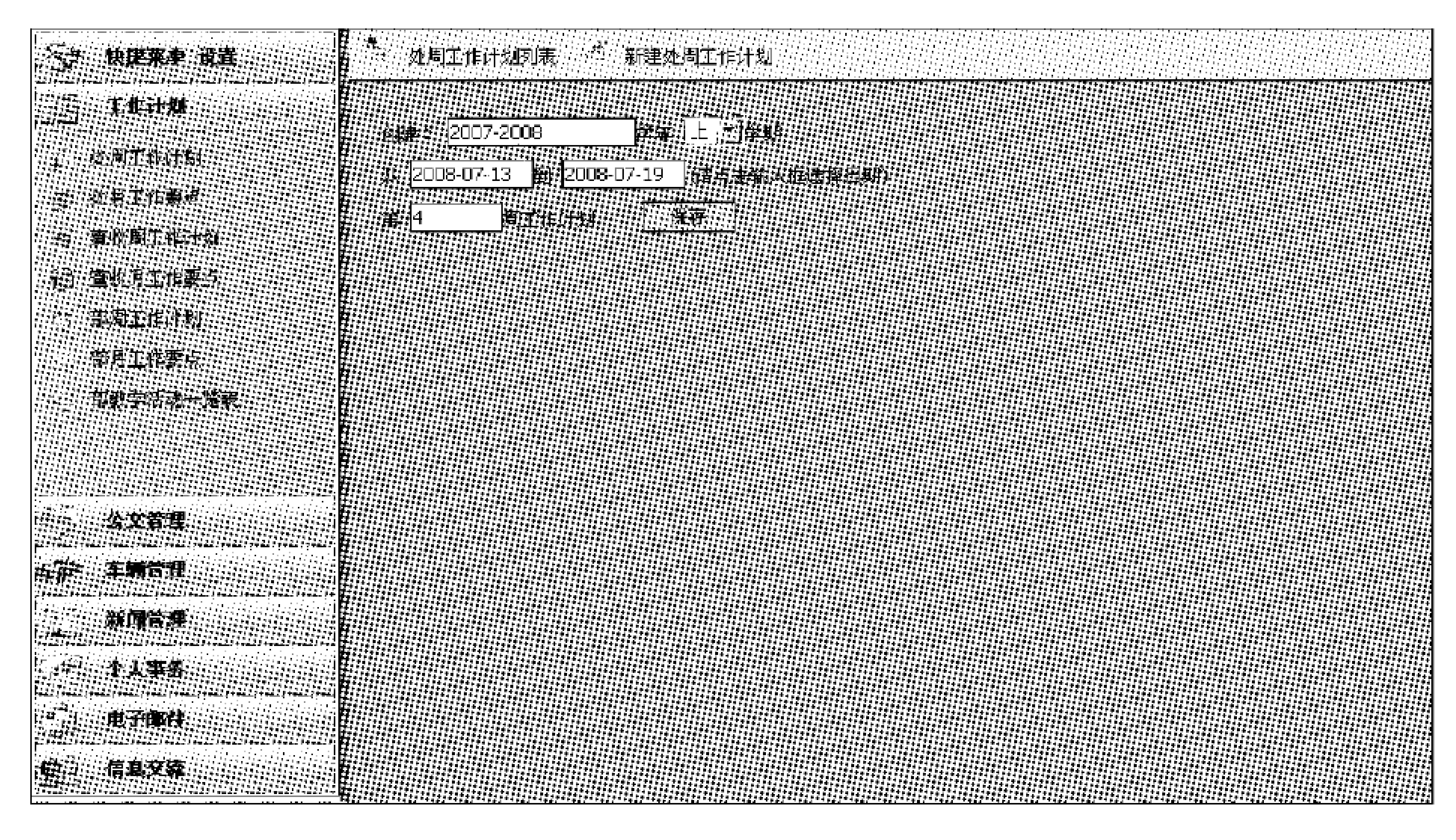


图 3-33　新建工作计划界面

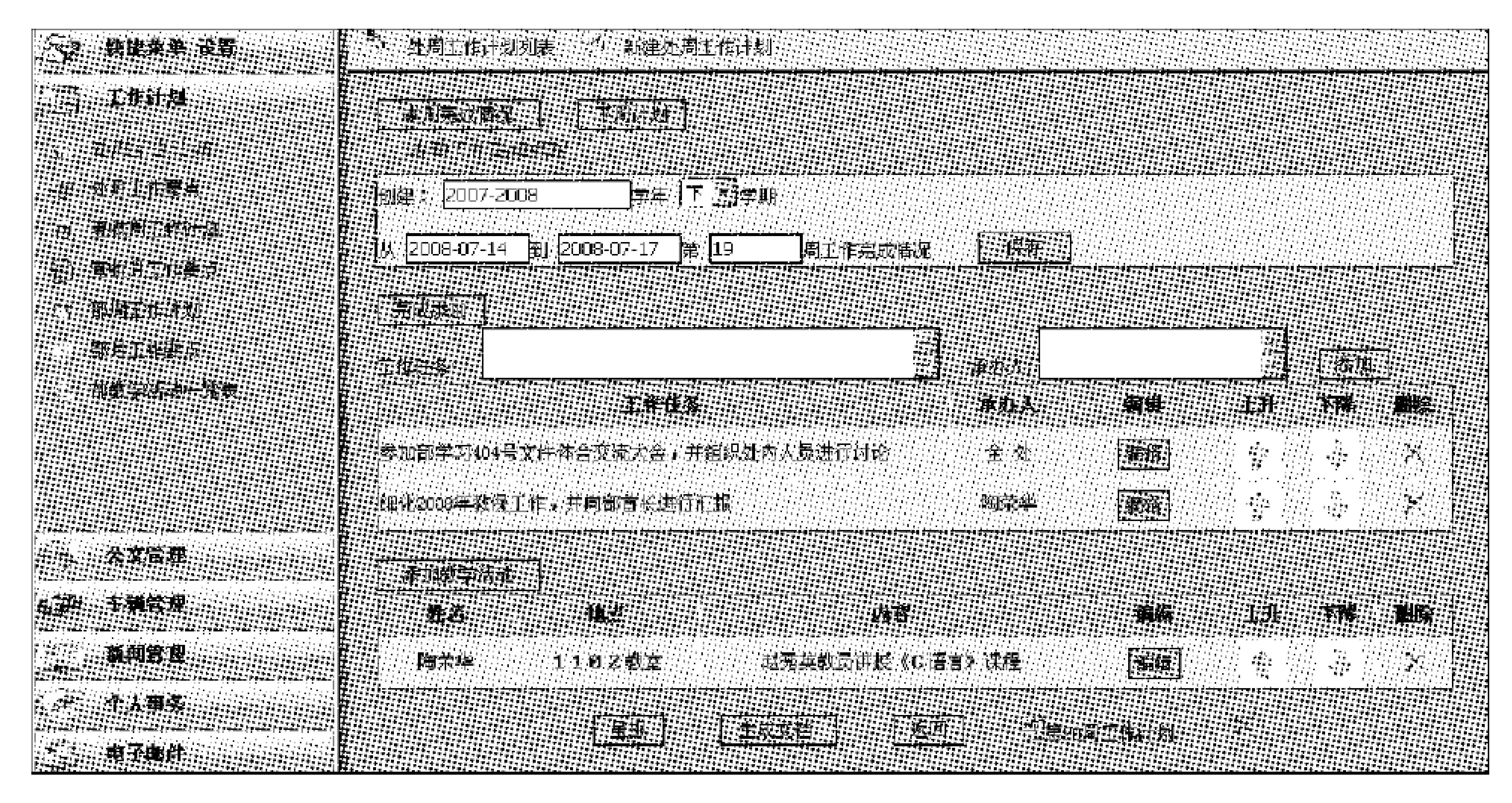


图 3-34　添加工作任务和教学条目界面

③ 新建处月工作要点。填写基本信息，浏览本地文件，单击"保存"按钮将在本地主机上编写好的月工作要点上传至服务器，如图 3-35 所示。

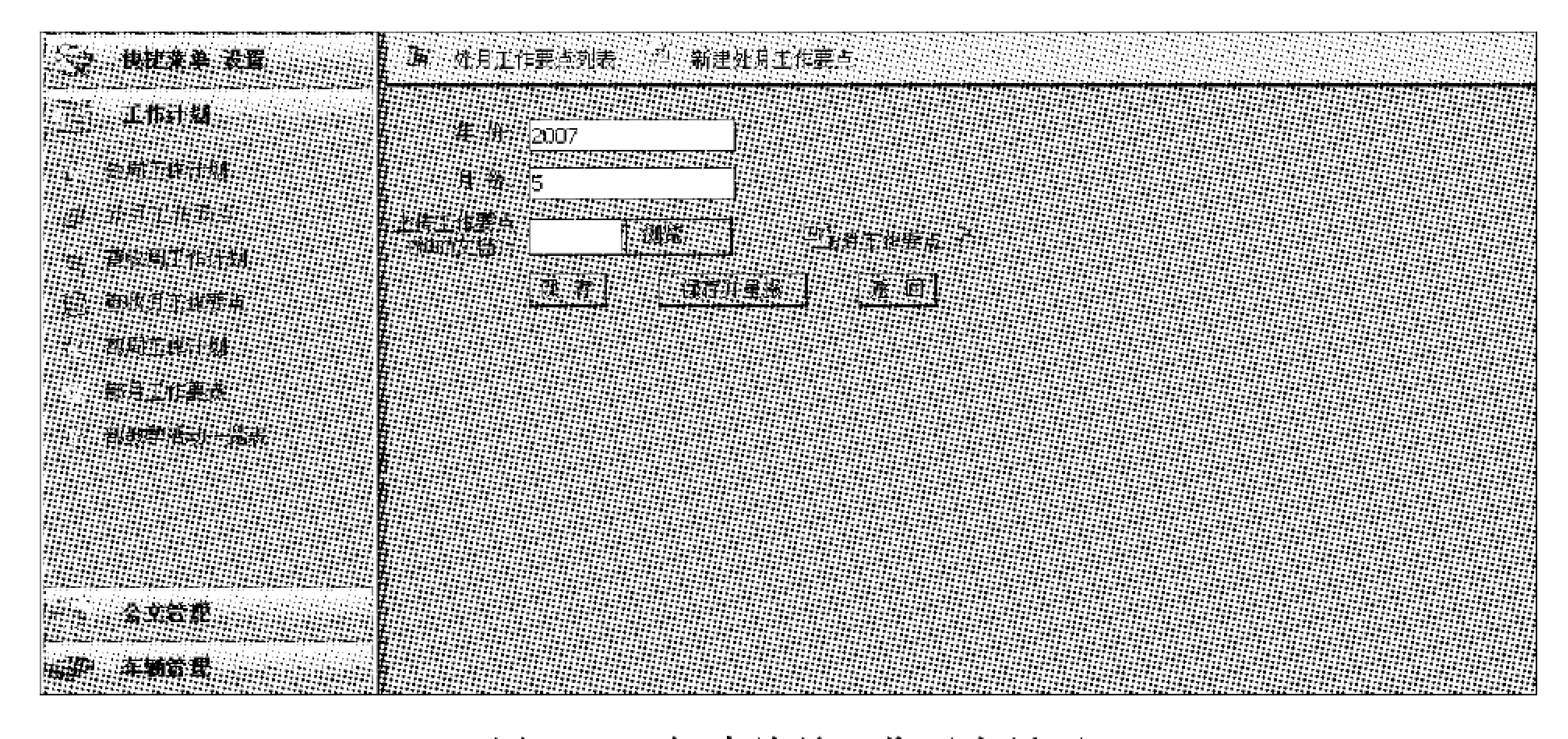


图 3-35　新建处月工作要点界面

④ 查收处周工作计划。在呈报的处周工作计划的列表中，单击相应的周次，进入到一篇工作计划中，然后单击列表中相应条目的“添加”按钮，将处本周完成情况的条目添加到相应的部周工作计划的本周完成情况中，而单击列表中相应条目的“添加重点”按钮或“添加日常”按钮，分别将处下周计划中的条目作为重点工作或日常工作添加到相应周次的部周工作计划的下周计划中。单击“打回”按钮打回工作计划。

⑤ 查收月工作要点。

## 2. 公文管理

(1) 呈批件管理

显示用户所具有权限查看的呈批件，可以对它们进行下载和删除操作，如图 3-36 所示。

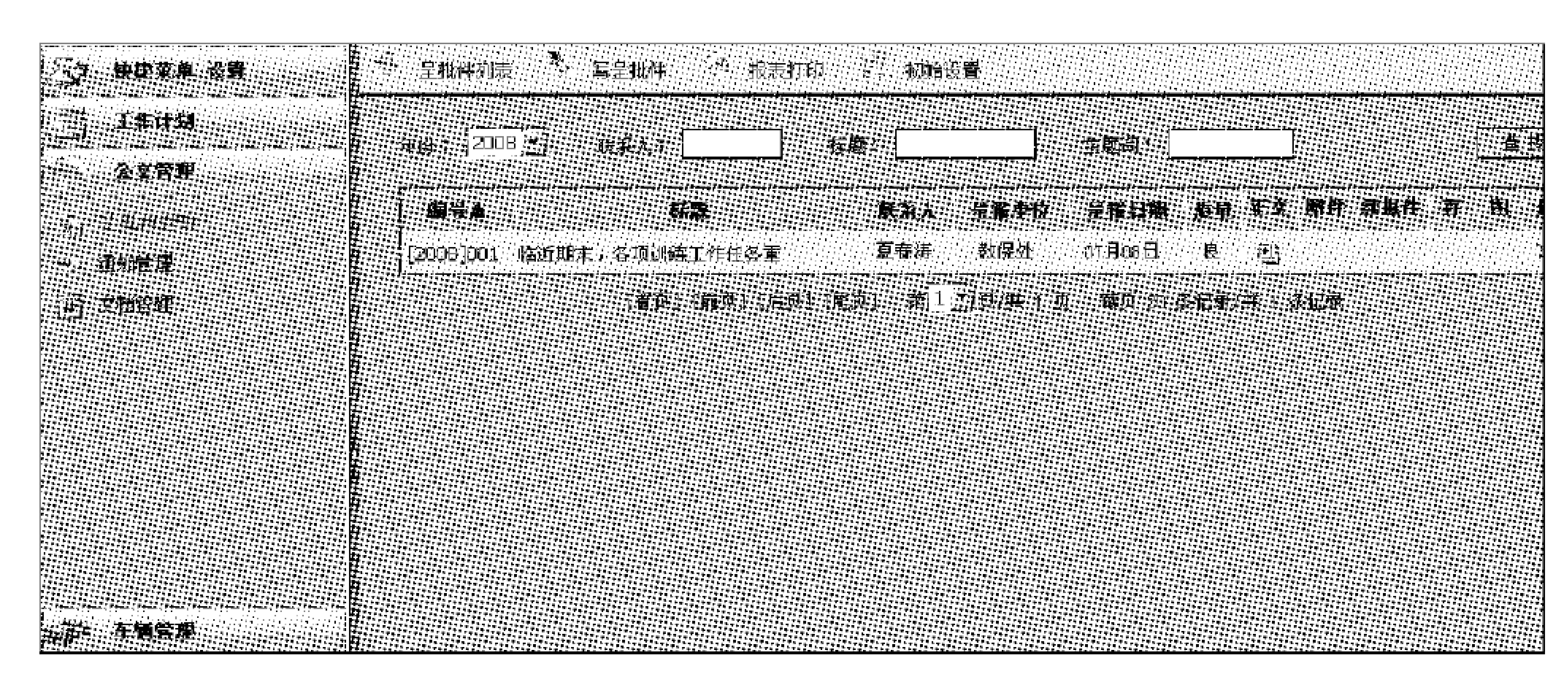



图 3-36　呈批件管理主页面

填写呈批件信息，保存后可生成 Word 文档，如图 3-37 所示。

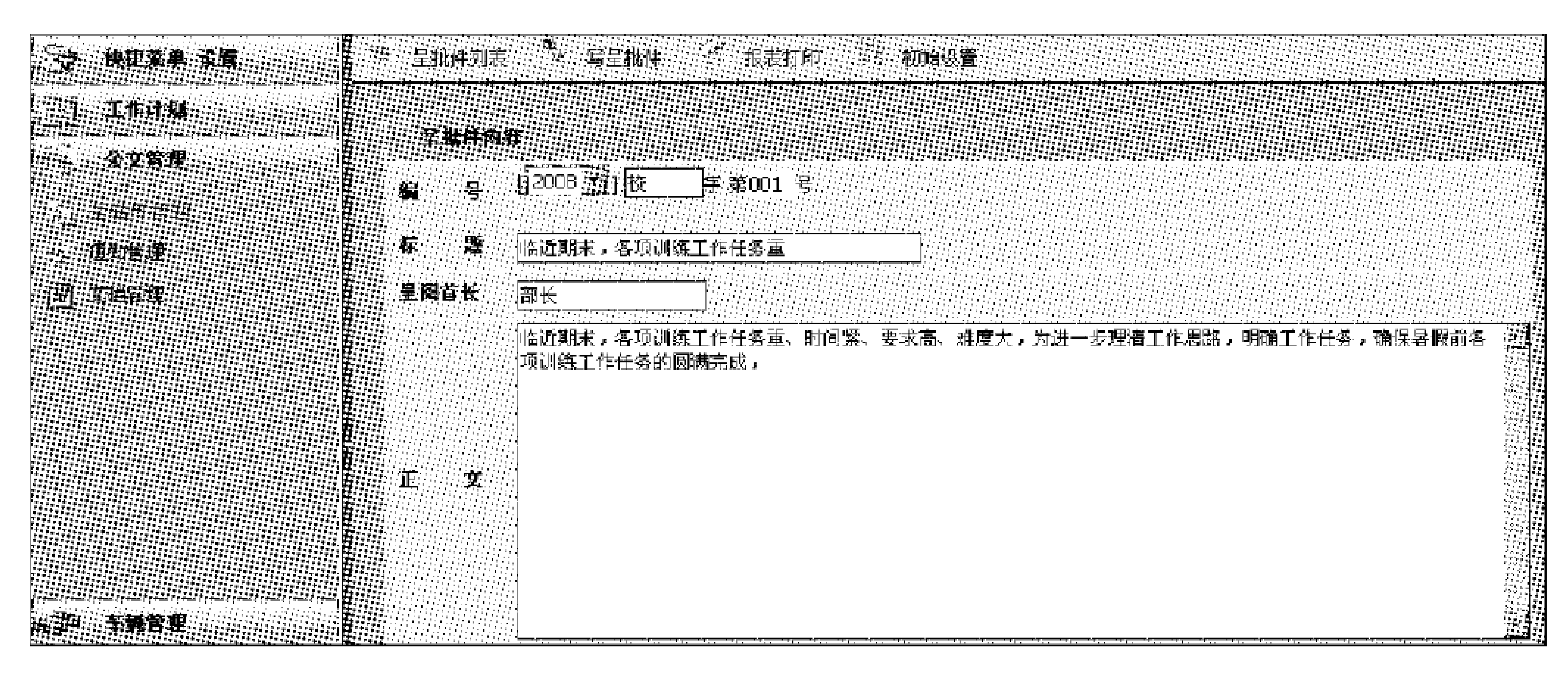



图 3-37　生成 Word 文档页面

(2) 通知管理

显示用户所具有权限查看的通知，可以对它们进行下载和删除操作，如图 3-38 所示。

(3) 文档管理

在文档管理页面，单击“新建”按钮，新建文件夹；单击“返回”按钮，返回上一级目录；

单击文档列表中的“重命名”按钮，进行重命名；单击列表中的“转发”按钮，进行文档的转发；单击“删除”按钮，进行文档的删除，如图 3-39 所示。

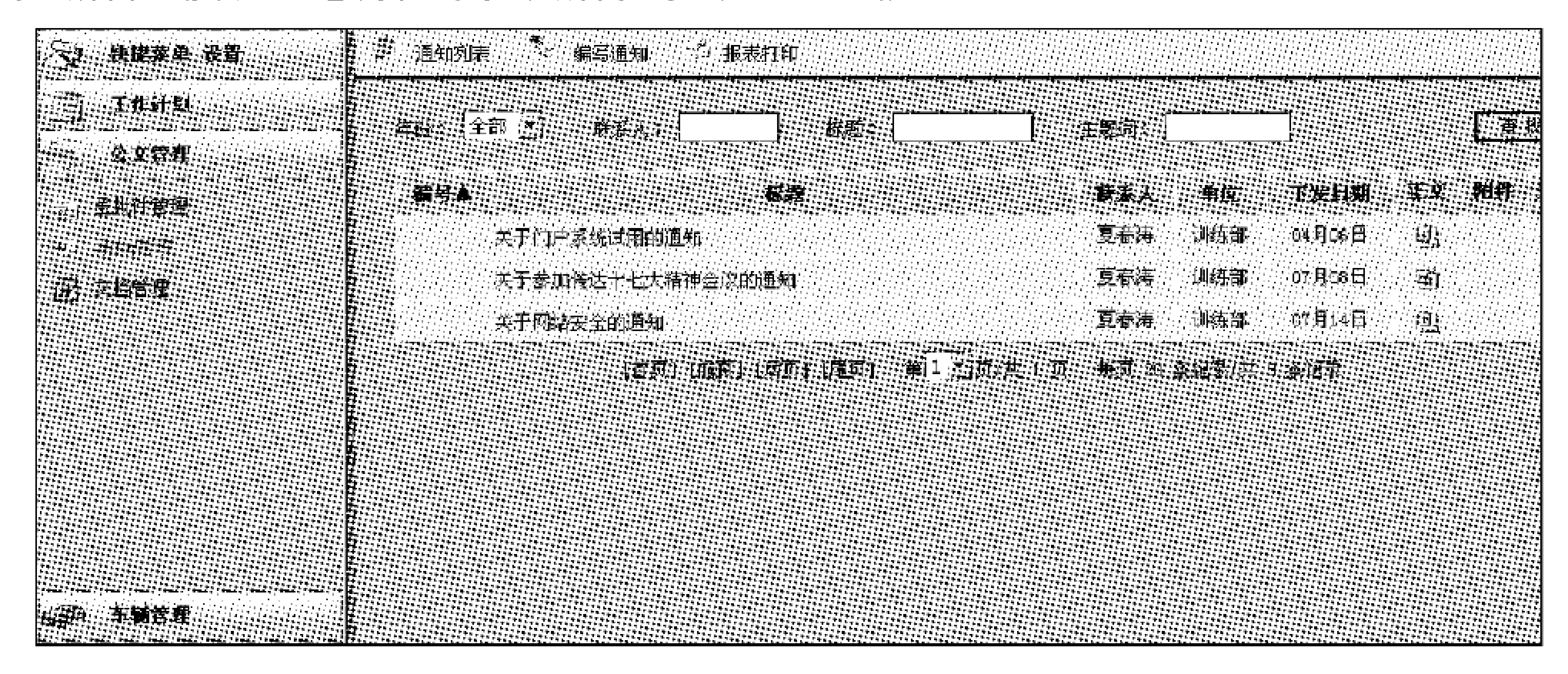



图 3-38　通知管理界面

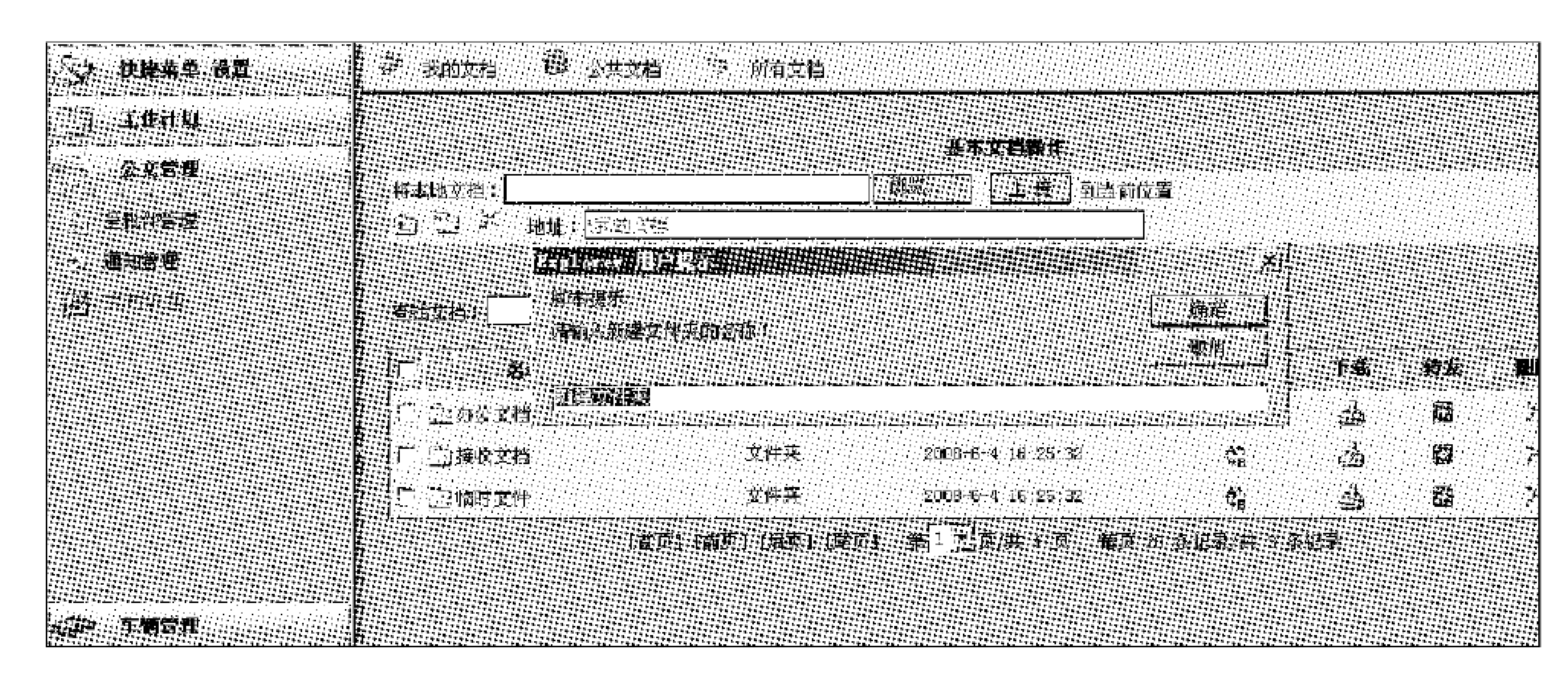



图 3-39　文档管理界面

### 3. 车辆管理

① 车辆信息查看、修改和删除。

② 出车申请。进入出车申请模块，显示当前可申请的车辆车牌号，提示用户填充申请车辆的相关信息。下方显示当前用户进行车辆申请的相关记录信息，单击某车辆的“详细”按钮，可看到该车辆申请的详细信息。

③ 派车管理。合法用户成功登录后，可对其所管辖的人员车辆申请请求进行审核。通过单击“批准”或“不批准”按钮，对相应的车辆申请进行审核，如图 3-40 所示。

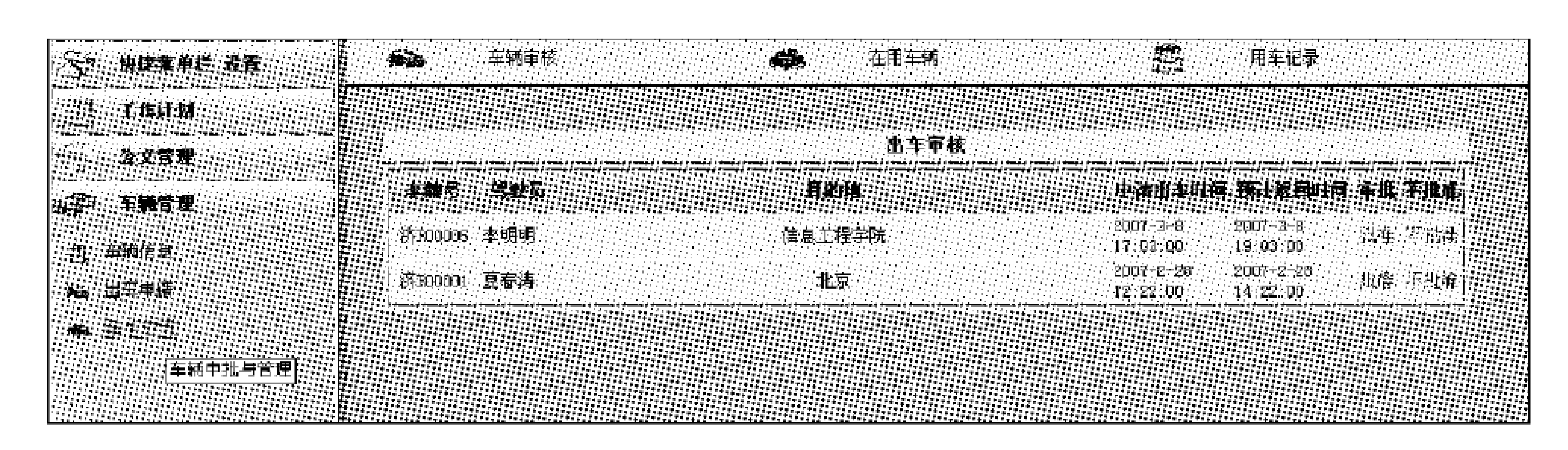



图 3-40　车辆管理界面



# 第4章 四级信息系统的安全设计和实现

## 4.1 安全功能和总体结构

### 4.1.1 安全功能

遵循GB 17859—1999的要求，基于形式化的安全策略模型，对系统内的所有主、客体进行标记，并实现强制访问控制；区分关键的安全部件和非关键的安全部件，明确定义部件之间的接口，且通过充分的测试和审核，体现结构化，通过结构化保障系统的安全功能有效。

### 4.1.2 总体结构

根据"一个中心"管理下的"三重保障体系"框架，构建安全应用平台，形成安全保护环境系统，该系统分为如下四个部分：计算环境、区域边界、通信网络和安全管理中心。其中计算环境又可细分为：Windows节点子系统、Linux节点子系统和典型应用子系统；而作为整个四级安全应用平台的核心，安全管理中心又可细分为安全管理子系统、审计子系统和系统管理子系统。

各子系统的主要功能如下所述。

(1) Windows节点子系统。对现有Windows操作系统进行安全增强，增加标记、强制访问控制、客体重用、可信路径等安全功能，增强身份鉴别机制的安全性，实现系统连接交互的结构化，使其部分满足GB 17859的四级要求，为信息系统的安全提供有效支撑。

(2) Linux节点子系统。对Linux操作系统进行结构化改造和安全增强，增加标记、强制访问控制、客体重用、可信路径等安全功能，增强身份鉴别机制的安全性，明确系统核心层、系统层以及应用层的边界，对各层之间的信息流进行安全检查，确保系统安全机制始终有效及不会被恶意篡改，使其基本满足GB 17859的四级要求，为上层应用系统的安全提供足够支撑。

(3) 区域边界子系统。对流入或流出安全保护环境的信息进行安全检查，增强其强制访问控制功能，确保安全保护环境的安全性不会受到破坏。

(4) 通信网络子系统。对安全保护环境间的信息流进行封装，确保信息在传输过程中不会被非授权窃听和篡改。

(5) 安全管理子系统。对安全保护环境中的计算节点、区域边界、通信网络、系统管

理的安全机制实施集中管理，包括标记管理、授权管理、策略管理等，为四级信息系统的安全提供基础保障。

(6) 审计子系统。对安全保护环境中的计算节点、区域边界、通信网络、安全管理、系统管理统一实施与安全相关的审计管理，包括制定审计策略、分析审计结果并作报警处理，为判断系统安全状态及应急处理提供依据。

(7) 典型应用子系统。安全保护环境为应用系统（如安全网站应用等）提供安全支撑服务。通过实施四级安全要求的网站应用，使用安全保护环境所提供的安全机制，为应用提供符合四级要求的安全功能支持和安全服务。

以上各子系统之间的逻辑关系如图 4-1 所示。

节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成了一个严密牢固的防护层，通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统机密性和完整性的安全，从而为典型应用子系统的正常运行和免遭恶意破坏提供支撑和保障。

区域边界子系统通过对进入和流出安全保护环境的信息流进行安全检查，确保不会有违背系统安全策略的信息流经过边界，它是四级信息系统的第二道安全屏障。

通信网络子系统通过对通信数据包的机密性和完整性进行保护，确保其在传输过程中不会被非授权窃听和篡改，使得数据在传输过程中的安全得到了保障，是四级信息系统的外层安全屏障。

安全管理子系统是四级系统的控制中枢，主要实施标记管理、授权管理及策略管理等。安全管理子系统通过制定相应的系统安全策略，并且强制节点子系统、区域边界子系统、通信网络子系统的执行，从而实现了对整个信息系统的集中管理，为重要信息的安全提供了有力保障。

审计子系统是系统的监督中枢，系统审计员通过制定审计策略，强制节点子系统、区域边界子系统、通信网络子系统、安全管理子系统、系统管理子系统的执行，从而实现对整个信息系统的行为审计，确保用户无法抵赖违背系统安全策略的行为，同时为应急处理提供了依据。

四级安全应用平台的总体流程可以分为安全管理流程与访问控制流程。安全管理流程主要由安全管理中心的安全管理员、系统管理员和系统审计员实施，且分别实施系统维护、安全策略部署和审计策略部署等机制。访问控制流程则在系统运行时执行，实施自主访问控制和强制访问控制等机制。

### 1. 策略初始化流程

节点子系统在运行之前，应首先由安全管理员、系统管理员和系统审计员通过安全管理中心为其部署相应的安全策略。其中，系统管理员首先需要为信息系统中的所有用户实施身份管理，即确定所有用户的身份、工作密钥和证书等，同时需要为信息系统实施资源管理，即确定业务系统正常运行需要使用的执行程序等。安全管理员需要通过安全管理中心为信息系统中所有主/客体实施标记管理，即根据业务系统的需要，结合客体资源的重要程度，确定其安全级，生成全局客体标记列表，同时根据用户在业务系统中的权限

和角色确定其安全标记，生成全局主体标记列表。在此基础上，安全管理员需要根据系统需求和安全状况，为主体实施授权管理，即授予用户访问客体资源能力的权限，生成访问控制列表和级别调整检查列表。除此之外，系统审计员需要通过安全管理中心中的审计子系统制定系统审计策略，实施系统的审核管理。

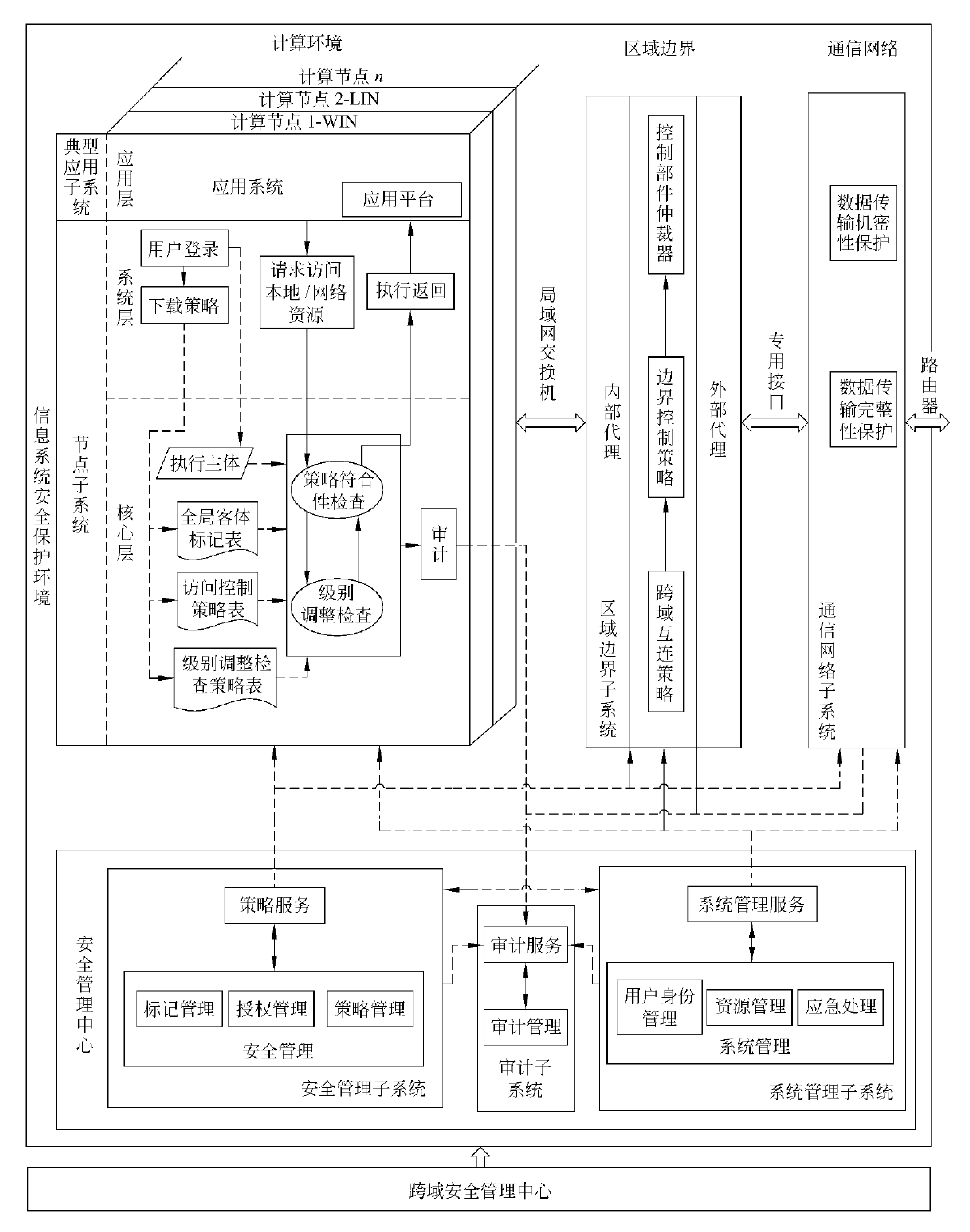



图 4-1 总体结构流程

### 2. 计算节点启动流程

策略初始化完成后，授权用户才可以启动并使用计算节点访问信息系统中的客体资源。为了确保计算节点的系统完整性，节点系统在启动时需要对所装载的可执行代码进行可信验证，确保其在可执行代码预期值列表中，并且程序完整性没有遭到破坏。计算节点启动后，用户便可以安全地登录系统。在此过程中，系统首先装载代表用户身份唯一标识的硬件令牌，然后获取其中的用户信息，进而验证登录用户是否是该节点上的授权用户。如果检查通过，系统将请求策略服务器下载与该用户相关的系统安全策略。下载成功后，系统可信计算基将确定执行主体的数据结构，并初始化用户工作空间。此后，该用户便可以通过启动应用访问信息系统中的客体资源。

### 3. 计算节点访问控制流程

用户启动应用后，应用代表用户发出访问本地或网络资源的请求，该请求将被操作系统访问控制模块截获。访问控制模块首先依据自主访问控制策略对其执行策略符合性检查，如果检查通过，那么该请求允许将被执行。否则访问控制模块将依据强制访问控制策略对该请求执行策略符合性检查。如果检查通过，那么该请求将允许被执行。否则，系统将对其进行级别调整检查，即依照级别调整检查策略，判断发出该请求的主体是否有特权访问该客体，如果上述检查通过，该请求同样允许被执行，否则，该请求将被拒绝执行。系统访问控制机制在安全决策过程中，需要根据系统审计员制定的审计策略，对用户的请求及决策结果进行审计，并且将生成的审计信息发送到审计服务器存储，供审计员检查和处理。

### 4. 接入控制流程

如果主体和其所请求访问的客体资源不在同一个计算节点上，该请求将会被可信接入模块截获，用来判断该请求是否会破坏系统安全。在进行接入检查前，模块首先通知系统安全代理获取对方节点的平台身份，并检验其安全性。如果检验结果是不安全的，则系统将拒绝该请求发生。否则，系统将依据强制访问控制策略，判断该主体是否允许访问对方节点的相应端口，如果检查通过，该请求将被放行，否则被拒绝。

### 5. 边界访问控制流程

如果主体和其所请求访问的客体资源不在同一个安全保护环境内，那么该请求必然会被区域边界控制设备截获并且进行安全性检查。检查过程类似于节点访问控制流程，不同的是，区域边界控制设备不仅接受本安全保护环境中安全管理中心的统一管理，而且需要接受上一级安全管理中心的管理，需要执行跨域互连策略，因此，区域边界从上一级安全管理中心下载策略，从跨域的角度检查是否允许该主体访问该客体资源。当检查通过后，该请求包将通过安全的通信网络传递到指定安全域中。

(1) 自主访问控制流程

系统在初始化过程中，安全管理中心需要对系统中的所有主体实施身份管理、授权管理和策略管理。其中身份管理是确定系统中所有合法用户的身份、工作密钥、证书等与安全相关的内容。授权管理是对用户提出的授予某主体访问某客体权限的请求进行批复的过程。策略管理是将授权信息生成自主访问控制策略，供节点系统执行。除此之外，系统

审计员需要通过安全管理中心制定系统审计策略，实施系统的审计管理。

系统初始化完成后，用户便可以请求访问系统资源，该请求将被自主访问控制模块截获。自主访问控制模块从用户请求中取出与访问控制相关的主体、客体、操作三要素信息，然后查询全局主体列表，得到主体所在用户组信息。进而依据自主访问控制策略对该请求实施策略符合性检查。如果该请求符合系统自主访问控制策略，则系统将允许该主体执行资源访问。否则，系统将直接拒绝该请求执行。

系统自主访问控制机制在执行安全策略过程中，需要根据系统审计员制定的审计策略，对用户的请求及安全决策结果进行审计，并且将生成的审计信息发送到审计服务器存储，供审计员管理，如图 4-2 所示。

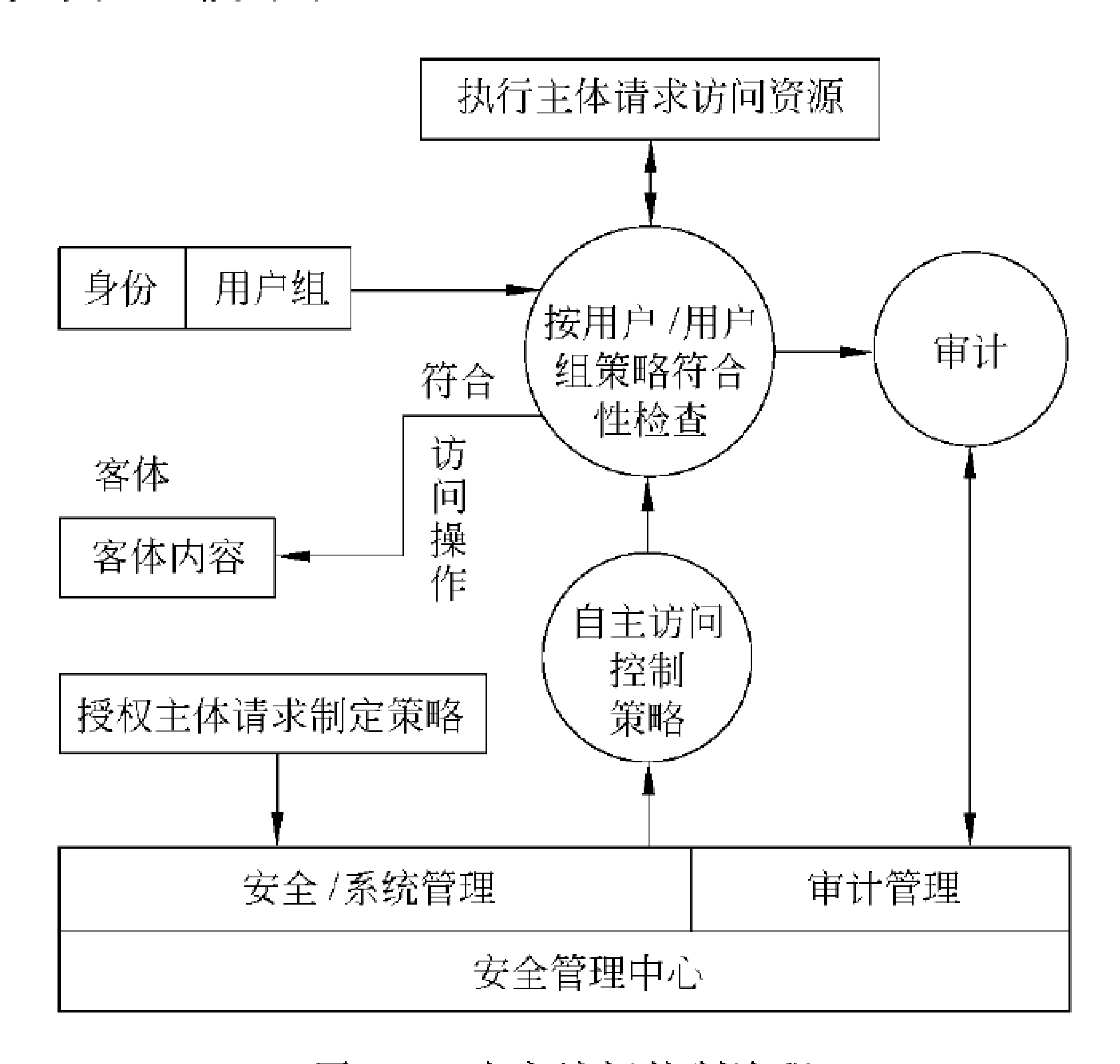



图 4-2　自主访问控制流程

(2) 强制访问控制流程

系统在初始化过程中，安全管理中心需要对系统中的所有主体和客体实施身份管理、标记管理、授权管理和策略管理。身份管理是确定系统中的所有合法用户的身份、工作密钥、证书等与安全相关的内容。标记管理是根据业务系统的需要，结合客体资源的重要程度，确定系统中所有客体资源的安全级，生成全局客体标记列表，同时根据用户在业务系统中的权限和角色确定主体的安全标记，生成全局主体标记列表。授权管理是根据系统需求和安全状况，授予用户访问客体资源能力的权限，生成强制访问控制列表和特权列表。策略管理则是根据节点系统的需求，生成和执行与主体相关的策略，包括强制访问控制策略、级别改变检查策略等，供节点系统执行。除此之外，系统审计员需要通过安全管理中心制定系统审计策略，实施系统的审计管理。

系统初始化完成后，用户便可以请求访问系统资源，该请求将被强制访问控制模块截获。强制访问控制模块从用户请求中取出与访问控制相关的主体、客体和操作三要素信息，然后查询全局主/客体列表，得到主/客体的标记信息。进而依据强制访问控制策略对该请求实施策略符合性检查。如果该请求符合系统强制访问控制策略，则系统将允许该主体执行资源访问。否则，系统将进行级别改变审核，即依据级别改变检查策略，判断发

出该请求的主体是否有特权访问该客体。如果上述检查通过，系统同样允许该主体执行资源访问，否则，该请求将被系统拒绝执行。

系统强制访问控制机制在执行安全策略的过程中，需要根据系统审计员制定的审计策略，对用户的请求及安全决策结果进行审计，并且将生成的审计信息发送到审计服务器存储，供审计员管理，如图 4-3 所示。

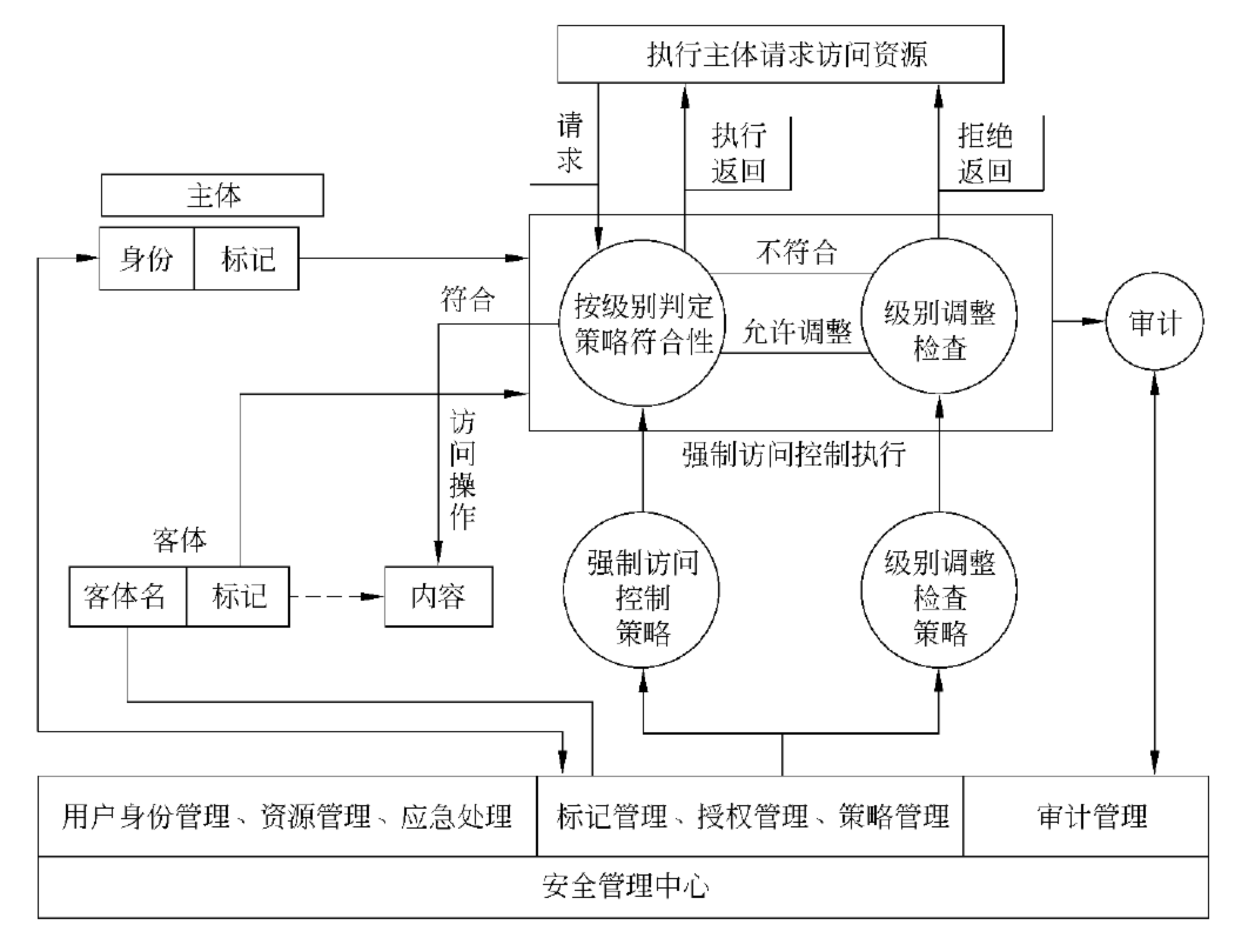



图 4-3 强制访问控制流程

(3) 子系统间接口

为了清楚描述各子系统之间的关系，将上述结构简化为图 4-4 所示的框图。方框表示各子系统，箭头表示各子系统之间的接口关系。

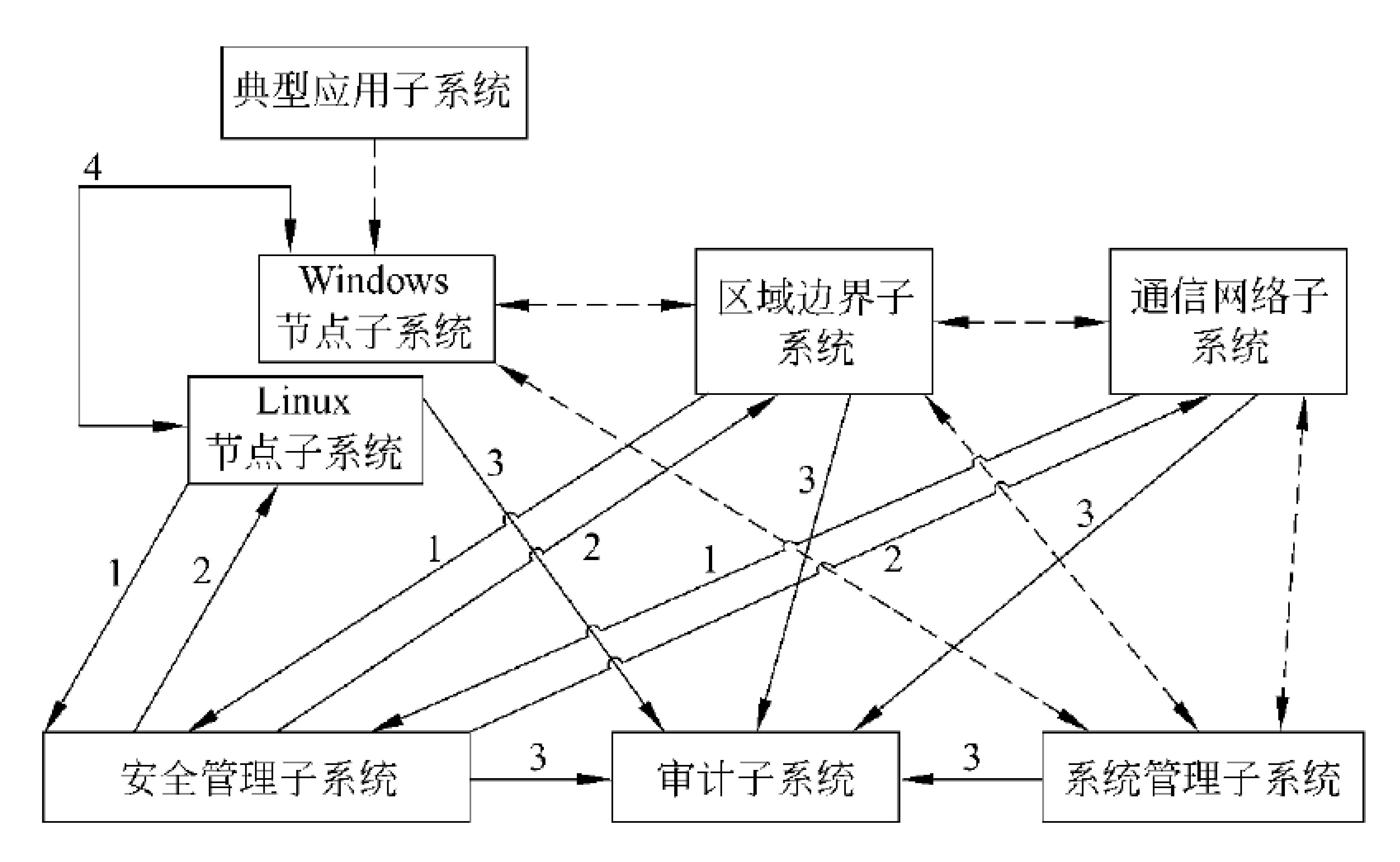



图 4-4 四级安全应用平台子系统接口

典型应用子系统与节点子系统之间通过系统调用接口，其他子系统之间则通过可靠的网络传输协议，按照规定的接口协议传输策略数据、审计数据以及其他平台认证数据等。由于不同子系统之间需要交换各种类型的数据包，于是需要明确定义子系统间的接口协议并规范传输数据包，使得它们能够透明交互，实现相应数据的交换。

## 4.2 实现方案和设备类型

### 1. 实现方案

第四级系统安全保护环境的实现方案是按照第四级系统安全保护环境的设计目标和设计策略，落实第四级安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计技术要求，选择符合相应要求的安全产品进行集成的。此外，系统安全集成还应包括配置系统备份与恢复机制，支持系统管理员在系统出现故障时进行恢复；根据应用对业务连续性的要求，配置系统级的本地和异地灾难备份与恢复机制，制定应急处置和灾难恢复预案，支持应急处理和恢复。

### 2. 设备类型

表 4-1 是第四级系统安全保护环境集成中各部分主要产品的设备类型。

**表 4-1 第四级系统安全保护环境主要产品的设备类型**

| 使用范围 | 产品设备类型 |
|---|---|
| 安全计算环境 | 操作系统、数据库管理系统、安全审计系统、终端安全管理、身份鉴别系统等 |
| | 操作系统等 |
| 安全区域边界 | 安全隔离与信息交换系统、安全网关等 |
| 安全通信网络 | VPN、加密机、路由器等 |
| 安全管理中心 | 安全管理平台 |

## 4.3 安全计算环境子系统的设计和实现

安全计算环境子系统分为 Windows 节点子系统和 Linux 节点子系统，下面分别进行描述。

### 1. Windows 节点子系统

满足 GB 17859—1999 规定的安全功能要求和保证要求，尤其是自身的结构化要求，具体的功能设计如下所述。

① 强制访问控制：支持二维标识模型的强制访问控制机制，能够保护信息系统的机密性及完整性不受破坏。

② 标记：对系统中的进程、文件进行全程标记，确保主客体在整个生命周期中其标记信息都是准确完整一致的。

③ 身份鉴别：有基于可信硬件设备的安全身份鉴别机制，且可以通过安全机制将身份与授权权限绑定。

④ 审计：对系统中所有违反安全策略的操作进行审计，并能阻止非审计管理员用户对审计信息的访问或破坏。

⑤ 数据完整性：通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。

⑥ 可信路径：建立用户与计算机信息系统之间的可信通信路径，确保该路径上通信信息的完整性不被破坏。

⑦ 可信链的建立与扩展：具有可信度量、可信存储及可信报告等可信功能，能够建立从操作系统到上层应用，最终到网络连接的完整信任链。能够确保操作系统的初状态可信，系统 TCB 的自身安全性不会遭到破坏。能够确保系统中的安全应用进程始终按照预期行为执行，其可信性不会遭到破坏。

⑧ 系统可信授权管理：提供细粒度的授权机制，使系统在制定安全策略时，可以逼近最小特权原则，并可以通过授权机制来对整个四级安全应用平台的安全权限提供连接。

⑨ 可信接入：接入信息系统的主机具有安全保障措施，终端平台环境对信息系统来说是可信的，主机之间的互连安全可靠。四级 Windows 操作系统通过安全增强，平台验证和加密信道通信实现主机之间的可信互连。

⑩ 四级 Windows 节点子系统主要是针对安全目的而开发，因此其指标的实现也主要是针对安全功能和安全保证而设置的，四级 Windows 节点子系统实现的功能指标见表 4-2。

**表 4-2 四级 Windows 节点子系统实现的功能**

| 指标类型 | 指标的具体内容 |
|---|---|
| 标记 | 提供三维标记，标记实体保密性级别、完整性级别和范畴。标记的对象包括系统中的用户、所有文件及进程。能够确保实体在整个生命周期中，其标记信息是准确完整一致的 |
| 强制访问控制 | 强制访问控制机制的实施与系统二维安全模型一致的安全策略，能够控制进程对文件的所有操作。强制访问控制机制应具有一定的灵活性，能够结合应用的流程，对进程不符合系统强制访问控制策略的行为进行检查，确保那些符合业务需求，但又不破坏系统安全的行为发生。强制访问控制机制始终有效，不会被旁路 |
| 身份鉴别 | 能够提供基于可信硬件设备的安全身份鉴别机制，确保非授权用户无法访问信息系统 |
| 审计 | 能够记录下述事件：用户登录事件、客体的创建和删除事件、安全管理员、安全审计员、系统操作员以及系统中其他用户的一切与安全相关的行为。审计的具体内容应满足 GB 17859—1999 中四级系统的审计规范要求 |
| 系统可信机制 | 能够确保系统 TCB、应用系统的完整性，确保恶意代码无法入侵系统和非授权终端无法接入信息系统 |

### 2. Linux 节点子系统

作为四级 Linux 系统，它不仅自身需要达到结构化保护的要求，还需要为整个四级安全应用平台提供支撑。具体的功能设计如下所述。

首先是安全功能要求，包括以下七点。

① 强制访问控制。支持二维标识模型的强制访问控制机制，并提供安全策略扩充的余地。

② 标记。对系统中的进程、文件进行全面标记，并可以将这一标记扩充到与其互联的所有 Linux 系统中。必要情况下，Linux 系统应能为特定的字段提供列表式的标识。

③ 身份鉴别。有基于可信硬件设备的安全身份鉴别机制，且可以通过安全机制将身份与授权权限绑定。

④ 审计。对系统中所有违反安全策略的操作进行审计，并能阻止非审计管理员用户对审计信息的访问或破坏。

⑤ 数据完整性。系统通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。

⑥ 可信路径。对用户的初始登录和鉴别，计算机信息系统在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

⑦ 安全封装。系统为系统环境上的应用提供安全封装机制，该机制控制应用的所有输入/输出信息和应用通过操作系统对资源的所有访问，并为通过分析应用输入/输出信息来确定应用对资源访问的安全策略提供操作系统上的功能支持。

其次是安全保证要求的功能设计，包括以下五点。

① 系统完整可信链的建立。从主机的 TPCM 模块和可信 BIOS 出发，通过可信链条的层层传递，保证系统初态的可信性，以及系统中各安全守护进程、安全应用进程的可信性及它们的可信启动。

② 系统访问控制机制的全面性。建立了一个基于二维安全策略模型之上的访问控制机制，并保证该控制机制遍及所有对文件的操作。

③ 安全程序结构化。结构化分解为关键保护元素和非关键保护元素，可信计算基必须建立在一个明确定义的形式化策略基础上，其接口也必须给出明确的定义，禁止从可信计算基关键保护元素到非关键保护元素安全策略的相关信息的流动。可信计算基的关键保护元素必须根据其保护原则划分功能层次，明确定义层次之间的调用关系接口，在不同层次之间建立全序或半序的函数调用关系，并通过分态等隔离措施保障层次关系的划分。

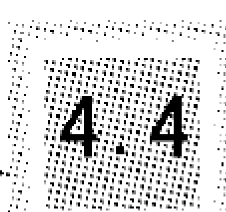
④ 重要接口参数结构化。通过系统可信计算基实施隔离，以防范系统的存储隐蔽通道。与可信计算基安全策略相关的敏感信息需要进行加密保护和校验措施，防止数据被窃取或被篡改。

⑤ 连接交互结构化。互相通过可信验证机制验证对方的可信性，确保互连部件的可信计算基可以无缝连接。

四级 Linux 节点子系统各安全功能和安全保证的具体实现功能指标见表 4-3。

表 4-3 高安全级别 Linux 操作系统功能指标

| 指标类型 | 指标项目 | 指标具体内容 |
|---|---|---|
| 标识 | 标识内容 | 提供二维标识,标识系统保密性级别、完整性级别和类别 |
| | 对进程的标识 | 系统进程自身携带二维标识,其标识与进程的当前用户安全级别和类别一致 |
| | 对文件的标识 | 系统所有文件有文件安全属性表或缺省安全属性。该文件安全属性表表征系统文件的二维标识<br>系统打开文件时,自动从文件安全属性表中读入对应的文件标识,并加载在文件数据结构、索引节点数据结构上 |
| | 网络信息安全标识 | 系统在发送网络信息时,应将二维安全标识附带发送,接收网络信息时,应能判断对方发来的二维网络信息安全标识 |
| | 授权标识 | 系统特定的可信主体可以给予特定的权限,并通过对可信主体的授权标识来表明这些特殊权限 |
| 强制访问控制 | 进程对文件的强制访问控制 | 系统进程对文件所有的系统调用均有强制访问控制机制,且这些机制实施的安全策略与系统的二维安全模型安全策略一致 |
| | 网络访问控制 | 系统对网络套接字的访问遵循系统的整体强制访问控制策略 |
| | 应用访问控制封装 | 系统对应用的输入/输出信息流具备过滤和格式检查功能<br>系统在系统调用层可以监控应用的所有系统资源的访问操作,并可以将根据格式检查所确定的应用安全策略部署到系统资源访问操作上,实现对应用的访问控制封装 |
| | 保密检查室与完整检查室 | 系统可对特定的、可确保其安全性的可信进程授予特权,保密检查室可允许不破坏系统保密性的特权进程的上读下写行为,完整检查室可允许不破坏系统完整性的特权进程的下读上写行为 |
| 系统可信机制 | 可信启动 | 系统通过可信计算机实现对可信引导程序的可信验证,防止外界对引导程序的任何篡改 |
| | 可信引导 | 可信引导程序可验证可信内核和可信初始盘的可信性,并把系统权限移交给安全内核和可信初始系统 |
| | 可信初始系统 | 可信初始系统中实现了系统安全模块加载和系统静态可信度量,并启动了可信守护进程 |
| | 可信守护进程 | 包括安全策略守护进程、可信互联守护进程和审计守护进程,提供系统的安全机制服务 |
| | 可信互联服务 | 通过可信服务守护进程提供部件间的可信互联服务,包括可信接入与远程可信证明 |
| 系统结构化保护 | 安全程序结构化 | 系统的 TCB 部分实现和其他部分的实现分离,TCB 部分全部在系统的内核态实施,并划分成核心层、系统层和驱动层,对核心层实施隔离和调用接口的检查 |
| | 重要接口参数结构化 | 对安全策略调用和审计信息发送等安全信息的处理,实施加密和完整性校验等数据的保护措施,保证安全数据的保密性和完整性 |
| | 连接交互结构化 | 四级信息系统各安全部件之间互联时,双方需要互相通过可信验证机制验证对方的可信性,确保互联部件的可信计算基可以无缝连接 |
| 系统审计机制 | 对强制访问控制机制的审计 | 审计信息能够通过探头对系统中所有访问控制行为提供审计功能 |
| | 审计策略实施 | 审计策略的实施可以根据审计级别设置,选择开启或关闭系统中特定的审计探头,或更改审计探头的审计触发条件 |



## 4.4　安全区域边界子系统的设计和实现

区域边界子系统是建立在安全信息系统之上的边界固化系统，根据安全管理平台所给定的访问配置策略，对所有跨边界访问的信息进行有效的安全访问控制。根据安全管理平台所给定的访问配置策略，对所有跨边界访问的信息进行有效的安全访问控制。保障网际信息交换在安全可控的环境下进行，对访问者进行身份验证，并保留可以追究直接责任人的审计信息。保障信息交换中所保护的安全域，不受其他非法访问的干扰和破坏。

区域边界子系统现采用三机系统体系结构：内部代理、仲裁系统和外部代理。仲裁系统和内外代理系统之间需要有安全可靠的数据传输通道，而且该数据传输通道需采用专有的数据传输协议；区域边界子系统需要获得访问主体及该主体所访问的客体信息，以对其进行访问控制。用户可以跨域访问客体，安全边界支持客体为 FTP 服务器保存的文件；Web 服务器保存的文件（网页或者文件）；邮件服务器保存的文件（邮件）；协议开放的私有文件交换 CS 结构服务。

其设计如下所述。

① 跨域访问控制：支持二维标识模型的强制访问控制机制，在跨边界访问时保护域中信息系统的机密性及完整性不受破坏。

② 跨域访问身份鉴别：基于安全管理策略的安全身份鉴别机制，通过认证机制将身份与授权权限绑定。

③ 审计：对经过边界的所有操作进行审计，并阻止非审计管理员用户对审计信息的访问或破坏。

④ 可信授权管理：只接受可信授权的系统管理，提供细粒度的授权机制，使系统在制定系统安全策略时，可以逼近最小特权原则。

⑤ 过滤：根据安全管理策略对信息进行一系列的安全过滤。

⑥ 可信接入：区域边界子系统的内部代理相对于所保护的安全域，也是其中的一子节点，因此也符合节点与节点之间的可信互联标准。

区域边界子系统主要是针对跨边界访问的安全目的而开发，因此其设计和实现的内容也主要是针对跨边界访问的安全功能和安全保证而设置。区域边界子系统跨边界访问实现的功能指标见表 4-4。

图 4-5 是区域边界子系统模块组成图，其中各模块功能描述如下：

① 应用代理子模块：开启服务监听代理，接收或发送跨域网络信息。

② 信息落地子模块：还原跨域网络信息至应用层，获取主体与客体信息。

③ 信息封装子模块：将允许通过的应用层数据，通过设定好的内部配置进行协议封装。

④ 跨域访问控制子模块：（强制访问控制功能）根据强制访问控制策略以及主客体标记信息，实现对所保护安全域中信息的强制访问控制，确保信息系统的机密性和完整性不受破坏。（身份鉴别功能）基于安全管理策略的安全身份鉴别机制，可以通过认证机制

**表 4-4 区域边界子系统功能指标**

| 指标类型 | 指 标 具 体 内 容 |
| --- | --- |
| 跨域强制访问控制 | 强制访问控制机制实施与系统二维安全模型一致的安全策略，能够控制进程对跨域文件访问的所有操作。并且应具有一定的灵活性，能够结合应用的流程，对跨域访问是否符合强制访问控制策略等行为进行检查，确保那些符合业务需求，但又不破坏系统安全的行为发生。跨域强制访问控制需要根据主体对跨域访问中文件、目录和设备的访问操作请求，根据安全策略对访问请求进行安全判定，对符合安全规则的请求，允许主体对资源的操作继续进行，反之则拒绝主体对资源的非授权访问 |
| 跨域访问身份鉴别 | 跨域访问身份鉴别机制应能够提供基于安全管理策略配置的安全身份鉴别机制，控制允许跨边界访问的机器以及用户。在允许访问列表中的机器及用户，认证通行；不允许的则终止非授权请求 |
| 审计 | 能够记录跨域访问行为中涉及到的一系列动作，包括对文件的添加删除、上传下载等操作。审计的具体内容需要满足 GB 17859—1999 中四级系统的审计规范要求 |
| 系统可信授权管理 | 只可接受可信授权的管理，安全策略的制定需满足最小特权原则 |
| 信息过滤 | 能根据安全管理策略对信息进行一系列的安全过滤，如文件类型是否符合、关键字过滤等 |
| 可信接入 | 区域边界子系统对于保护的安全域来说也相当于其中的一个安全节点，因此需要满足节点与节点之间的可信接入。具体内容参照安全节点子系统中的说明 |

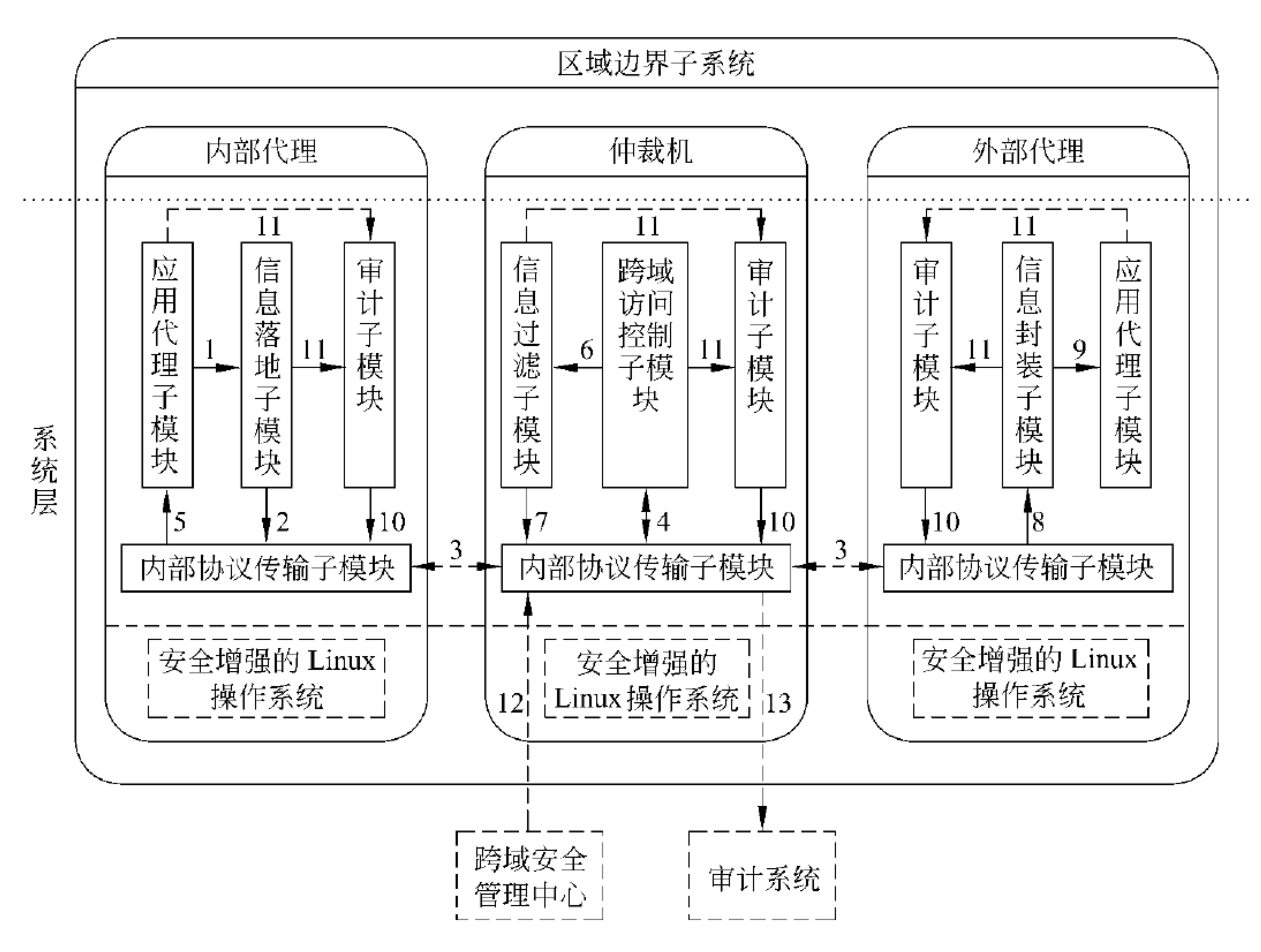



图 4-5 区域边界子系统模块组成

将身份与授权权限绑定。

⑤ 审计子模块：对经过边界的所有操作进行审计，并向审计服务器提交审计信息。

⑥ 信息过滤子模块：根据安全管理策略对信息进行一系列的安全过滤。

⑦ 内部协议传输子模块：三机内部之间的数据传输。

## 4.5　安全通信网络子系统的设计和实现

负责保证安全系统在通过网络进行跨域访问时的安全，其具体设计和实现如下所述。

① 数据源身份认证：证实数据报文是所声明的发送者发出的。

② 数据完整性：证实数据报文在传输过程中没被修改过，无论是被故意改动过还是发生了随机的传送错误。

③ 数据的机密性：隐藏明文的消息，通常靠加密来实现。

④ 防止重放攻击：当攻击者将截获到的数据报文在稍后的时间内发送时，会被检测到，并丢弃。

用 IPSec 对数据包进行加密和验证，密钥也是通过强壮的 IKE 协商的，因此可确保数据包的机密性和可信性。同时，IPSec 对数据包进行封装，隐藏数据包的一些通信特征，可抵抗通信分析。为了在不同的安全域中的透明通信，将该设备作为网关部署，这样就可以在安全保护环境之间实现安全通信，同时不影响内部的信息交换。

系统采用硬件加密卡进行加解密运算，加快了运算速度，也增强了安全性。加密卡是以 PCI 或者专用的接口插在主板上，在处理数据包时，模块根据密码卡要求的格式将数据包重新组织，同时告诉加密卡加密算法和密钥等信息，由硬件自动实现对数据包的加解密操作，从而提高性能和安全性。

VPN 网关的主要功能模块包括策略管理、密钥交换、加密库模块、报文封装模块、加密卡驱动。子系统的组成框图如图 4-6 所示。

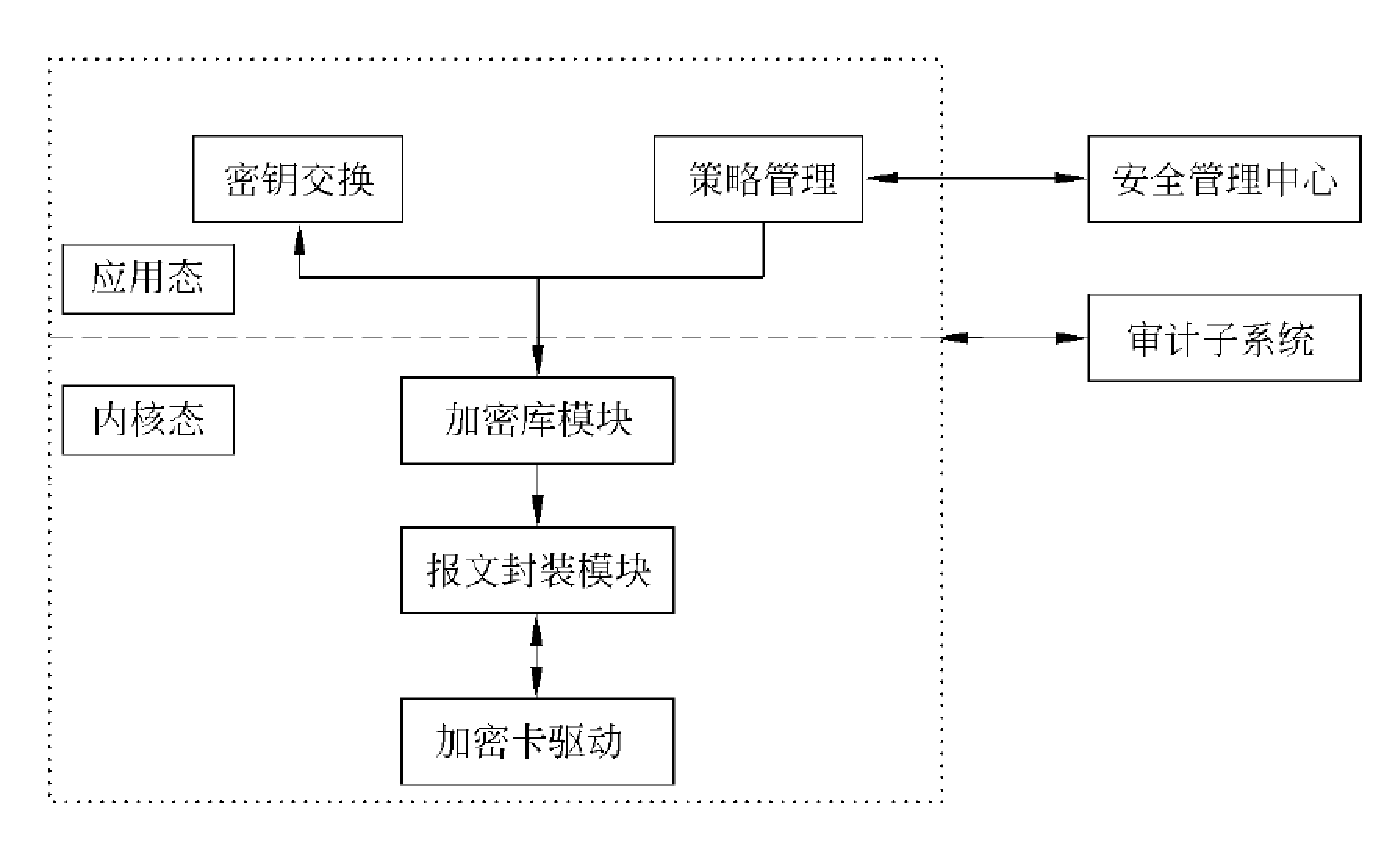



图 4-6　网络通信子系统模块组成

### 1. 策略管理

从安全管理中心下载安全策略，设定 IPSec 的算法以及密钥协商和密钥的存储位置等。

策略维护通过配置文件来实现。即用户对策略配置和管理系统进行操作，实际上就是操作配置文件，但用户配置的只是配置文件中的一部分，配置文件中的其他内容不允许用户修改，其中包括：

① CA 证书、用户证书和私钥的存放位置。CA 证书是由 CA 中心负责发放的，该证书用智能卡形式发放，另外还支持由第三方提供的证书来进行认证。

② 采用 ESP 协议时，第一阶段和第二阶段的加密算法、散列算法和认证算法。

③ 连接形式：对于网关与网关之间的通信，网关总是主动连接，即 IKE 主动发起协商，试图和对方进行安全协商，重传三次后不成功就放弃。对于网关与主机的通信，网关是被动连接，即网关只有在接收到主机的协商消息后才和主机进行协商。

其他选项采用 IKE 里面的默认配置，如重传次数、最大交换时间等。

### 2. 密钥交换

密钥交换模块作为一个服务运行，负责处理用户的管理配置命令，同对方设备进行密码协商交互、密钥载荷的加密验证处理以及同 IPSec 内核的安全联盟数据库 SA 的交互。

### 3. 密钥库模块

IPSec 内核主要包括以下几个功能：完整实现 AH/ESP 协议、维护策略库(SPD)、维护安全联盟 SA(Security Association)。在结构图中包括密钥库模块和报文封装模块。密钥库模块实现了上面的 SPD 和 SA 部分，它决定 IPSec 服务所使用的算法并放置服务所需密钥到相应位置。

IPSec 驱动模块在系统内核运行，支持传输模式和隧道模式两种安全工作模式。完成 AH 协议和 ESP 协议处理，按照 IPSec 协议标准对适当的数据包进行封装和解封操作。实现安全关联库和安全策略库，具有与 IKE 服务程序的通信接口，能够响应 IKE 服务程序的命令消息，刷新安全关联库的内容，同时也能够向 IKE 服务程序发送命令请求信息。实现验证算法和加密算法，提供算法的 API 调用接口。

可以把 IPSec 看作是位于 TCP/IP 协议栈的下层协议。该层由每台机器上的安全策略和发送、接受方协商的安全关联 SA 进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的 IP 地址，协议和端口号满足一个过滤机制，那么这个数据包将要遵守关联的安全行为。

### 4. 报文封装模块

该模块具体实现 IPSec 功能的 ESP 协议处理。从 SA 中得到加密算法和密钥，对数据包进行组织，把需要加密的报文以及加密算法、加密密钥等传送到加密卡驱动，由加密卡完成加解密操作。当加解密操作完成后，取出报文，并将报文按照既定的策略发送。

### 5. 加密卡驱动

加密卡启动及初始化后，加密卡驱动可管理用户提交的宏指令，驱动会将 IPSec 内核

模块下发的各种命令提交加密卡执行。然后加密卡负责解释和执行用户发出的命令，且返回该命令的执行状态。

## 4.6 安全管理子系统的设计和实现

安全管理子系统包含主客体标识管理、授权管理、策略管理等部分，是四级安全应用平台安全策略部署和控制的中心，其部署的安全策略则是连接各安全部件和各安全保障层面的纽带。

其具体的设计如下所述。

① 提供用户标记管理功能，为系统中的各用户配置安全级别和安全范畴。

② 提供客体标记管理功能，为系统中与安全业务相关的客体设定安全标记。安全标记包括与文件名直接相关的安全标识、目录安全标识、通配符格式的安全标识等类型。同时提供安全标识中安全级别的修改接口，供人工参与安全级别的制定和更改。

③ 提供授权管理界面，安全管理子系统提供授权模板维护强制访问控制表和自主访问控制表，将对特定客体的读、写执行等权限赋予相应的用户。对应用流程的特定位置进行授权，制定等级改变策略、网络访问控制策略等。

安全管理子系统的实现如下所述。

① 生成访问策略库。访问策略库是将用户与用户能够访问的客体资源结合起来所形成的一个访问控制策略表，目前使用 BLP 策略模型、Biba 策略模型和二维标识策略模型，安全管理子系统根据应用的安全策略配置，生成访问策略设置，并将访问策略设置与策略配置功能所生成的用户身份配置、文件标识配置以及可信接入策略和可信进程名单等组装发送到各安全部件中。

② 策略请求和处理。策略请求和处理是将设定客体安全级别的特权和该特权所授予的用户身份结合起来所形成的一个特权列表，该列表项目来源于各用户提出的主客体安全级别修改请求和自主访问控制策略申请，反映待定安全级别的客体资源属性和可定级主体范围，并将该列表发放到相应拥有定级权限的主体。

根据上述的安全功能要求，安全管理子系统的实现指标见表 4-5。

**表 4-5 安全管理子系统实现指标**

| 指标类型 | 指标项目 | 指标具体内容 |
|---|---|---|
| 标识管理 | 主体标识管理 | 为用户提供直观的配置界面，配置包括用户身份对应的安全级别、用户属性等信息<br>能够检查用户属性和安全级别的合规性 |
| | 客体标识管理 | 提供模板编辑方式的应用文件标识管理，模板提供一组文件标识方法，其中文件名的部分字段可以用变量方式表示，由管理子系统为变量赋值，变量表示应用的具体部署方法，包括应用部署机器、目录、配置等信息<br>标识管理配置界面也可以直接对文件进行标识配置，包括文件的安全级别、完整性级别和范畴 |

续表

| 指标类型 | 指标项目 | 指标具体内容 |
|---|---|---|
| 授权管理 | 授权管理 | 以手工编辑的方式生成强制访问控制列表、自主访问控制列表、特权列表文件(特权列表文件和应用所需特权相对应),并提供授权管理界面,由安全管理员决定特权应授予哪个用户<br>执行特权授予时,应能够检查支撑应用执行的必要特权是否全部授予相关用户,并可以检查特权所授予的用户是否拥有获取该特权的权限 |
| 策略管理 | 策略文件的生成和下发 | 安全管理子系统维护一个访问策略数据库,存储用户权限、客体标识的各种信息,并可以根据访问策略设置情况,与可信网络连接和可执行代码预期值策略等组装,为每台机器生成访问策略配置文件<br>安全管理子系统可以通过密码协议保护的网络通信将对应机器的访问策略配置文件发送给各机器的安全操作系统环境 |
| | 策略请求处理 | 安全管理子系统接收和存储用户提出主客体标记申请和安全策略请求的各种信息,并可以转交给特权机构(用户)审核和批复<br>安全管理子系统可以通过密码协议保护的网络通信将对应机器的策略请求发送给安全管理子系统,而安全管理子系统通过代理发送给定级机构处理并返回处理结果 |

安全管理子系统分为安全管理界面子模块、授权管理子模块、标记管理子模块、策略管理子模块、审计管理子模块、策略下载请求处理模块,以及策略请求处理子模块。结构如图 4-7 所示。

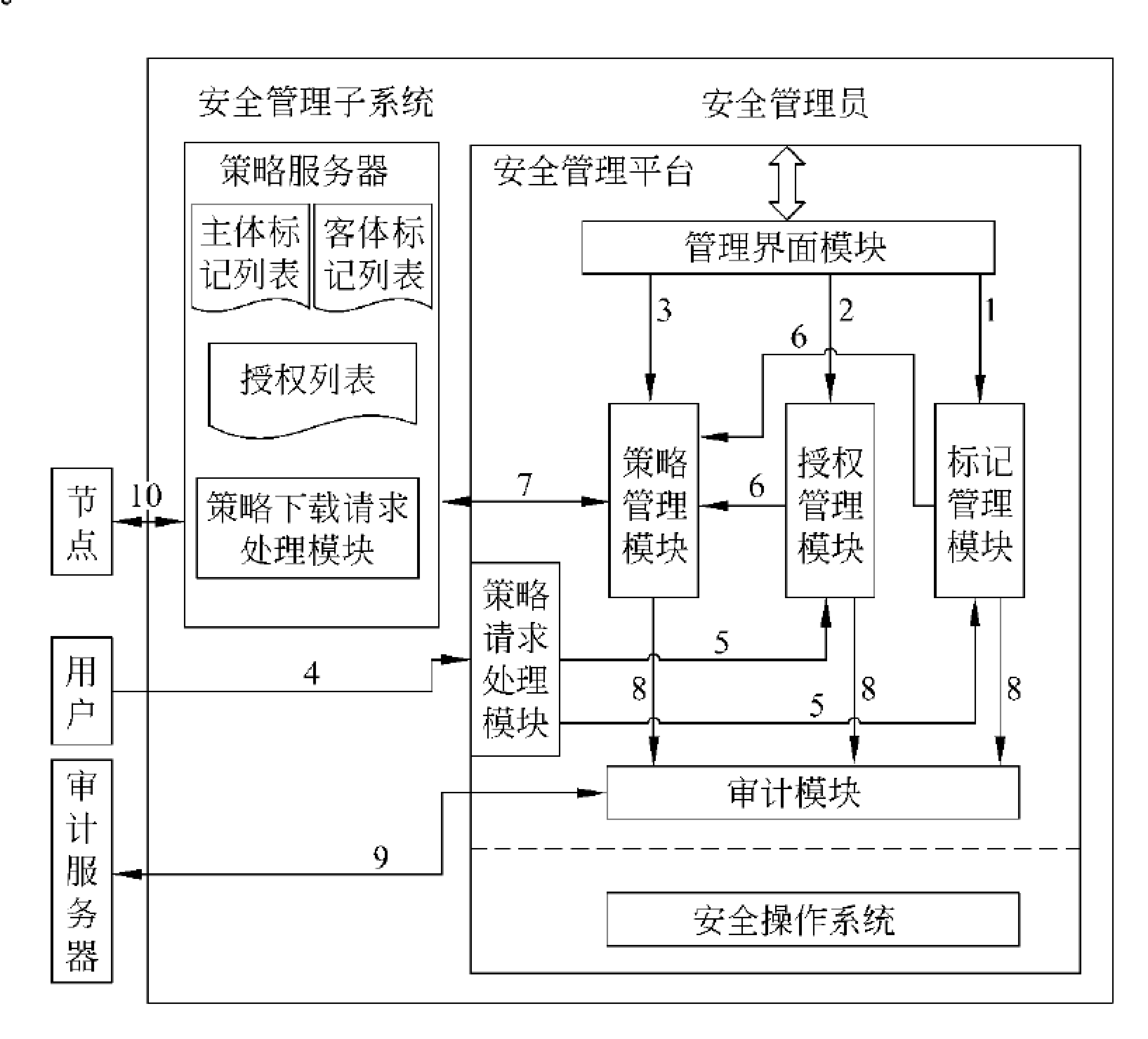



图 4-7 安全管理子系统模块结构

安全管理子系统需连接到系统环境中。安全管理界面子模块为安全管理员提供各项安全管理功能配置接口,根据三权分立原则体现安全管理员所拥有的权限和职责。授权

模块完成对用户相关权限的管理，标识管理模块负责安全管理中心所辖的所有主客体资源的标记，策略管理子模块提供的接口函数负责安全策略的制定和维护，同时负责安全策略服务器的管理和维护。策略请求处理模块接收主客体标记和授权请求信息，然后将请求用户提出的策略请求信息转发给特权用户或特权机构，由这些特权用户对客体安全标识进行设定，返回给策略请求处理模块，然后提交给策略管理模块完成策略服务器中策略内容的更新；安全策略由策略服务器的策略下载模块发送给安全管理子系统管辖的节点、区域边界和网络设备。安全管理员的操作行为被审计模块记录并发送给审计服务器。

## 4.7 审计子系统的设计和实现

审计子系统用于存储和处理总系统中的所有审计信息，审计员可以在安全管理中心上查看审计信息，其设计和实现如下所述。

① 生成审计策略并发放。使用安全管理中心提供的审计策略设置界面，使审计管理员可以选择四级安全应用平台不同范畴中的主客体访问审计级别，并与访问策略、等级检查策略相配合，生成具体的审计策略，将该策略发放给对应的安全部件。

② 接收、存储审计信息。接收从安全部件传来的审计信息，并进行存储和处理。

③ 查询审计信息。使用安全管理中心提供的审计界面将审计信息直观地提供给安全审计员，并提供简单的审计信息分类查询功能。

审计子系统实现的功能指标见表 4-6 所示。

表 4-6 审计子系统实现的功能指标

| 指标类型 | 指标项目 | 指标具体内容 |
|---|---|---|
| 审计管理 | 审计策略的生成和发放 | 审计策略配置界面，对系统中不同范畴的审计级别进行设置<br>审计子系统可以根据审计级别和应用安全策略，确定所要审计的具体操作情况，为各台机器生成审计策略配置文件<br>审计子系统可以通过密码协议保护的网络通信将对应机器的审计策略配置文件发送给各机器的安全操作系统环境 |
| | 审计信息的浏览和查询 | 审计子系统可以通过密码协议保护的网络通信接收对应机器的审计信息<br>审计子系统可以根据日期、范畴、审计级别向安全管理中心提供审计信息查询 |
| | 审计信息的接收 | 审计子系统可以接收其他子系统的审计信息，并进行存储 |

审计子系统由节点审计代理模块、审计服务器、审计信息查询模块、审计策略管理模块、审计信息分析模块组成，如图 4-8 所示。

节点审计代理模块向审计服务器发送审计信息，并接收审计服务器下发的审计策略，供节点子系统、边界子系统、网络子系统和安全管理中心子系统等使用。

审计服务器：接收节点审计模块发来的审计信息，进行存储和使用，接收审计查询模块的查询请求，并返回查询结果；接收审计策略配置模块的策略配置信息，修改审计策略。

审计信息查询模块：向审计服务器发送查询信息，并接收查询结果，供安全管理中心显示。

审计信息分析模块：对重要审计信息进行分析并报警。

审计策略管理模块：向审计服务器发送策略配置信息。

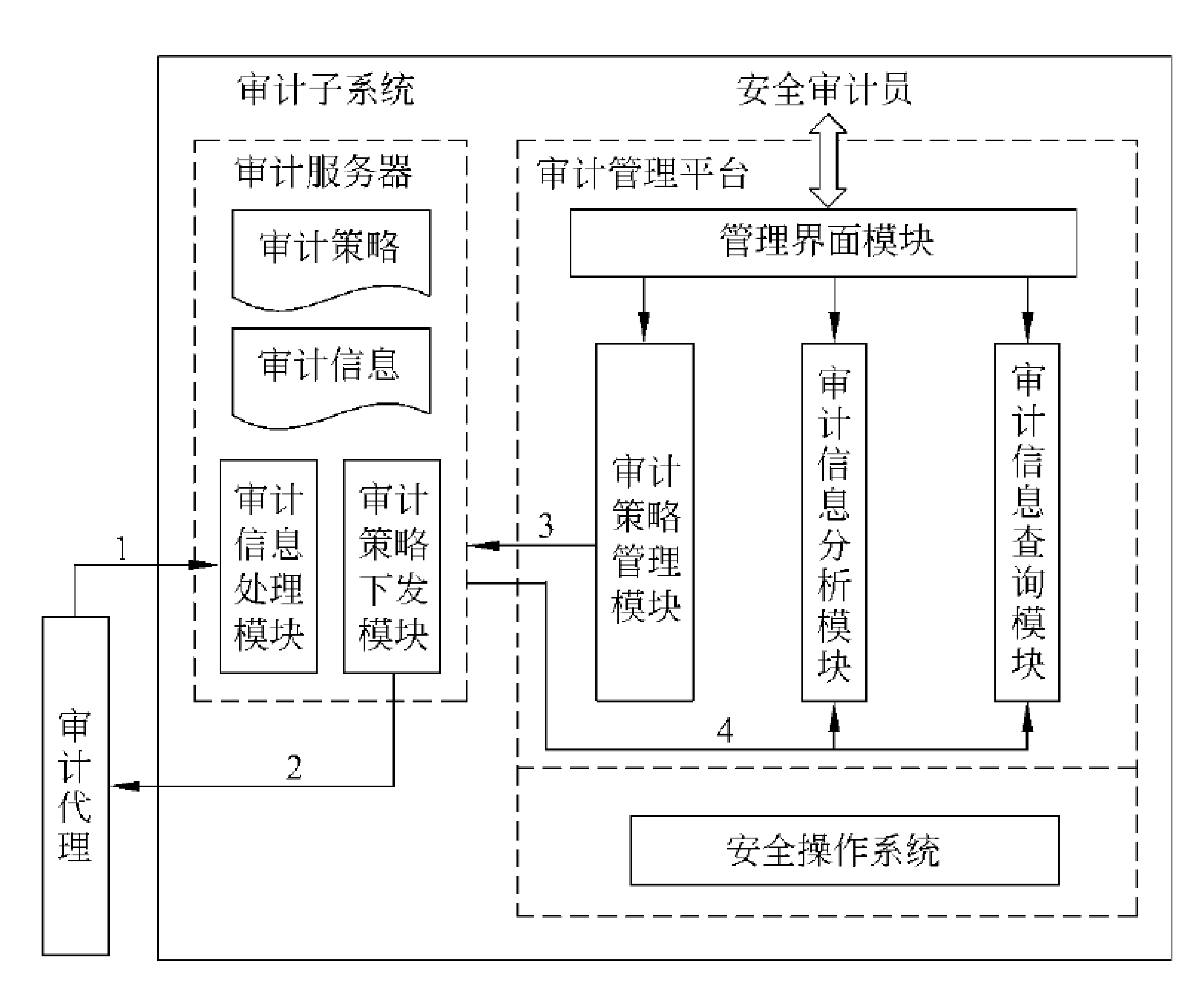
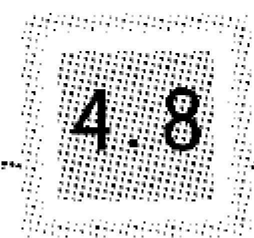



图 4-8　审计子系统模块结构



## 4.8 典型应用子系统的设计和实现

网站防护子系统由恶意代码主动防御模块、网页文件过滤驱动模块、SQL 注入过滤模块、网络行为监测和审计模块、网络服务应用区域边界防护模块和安全管理中心模块六部分组成，如图 4-9 所示。

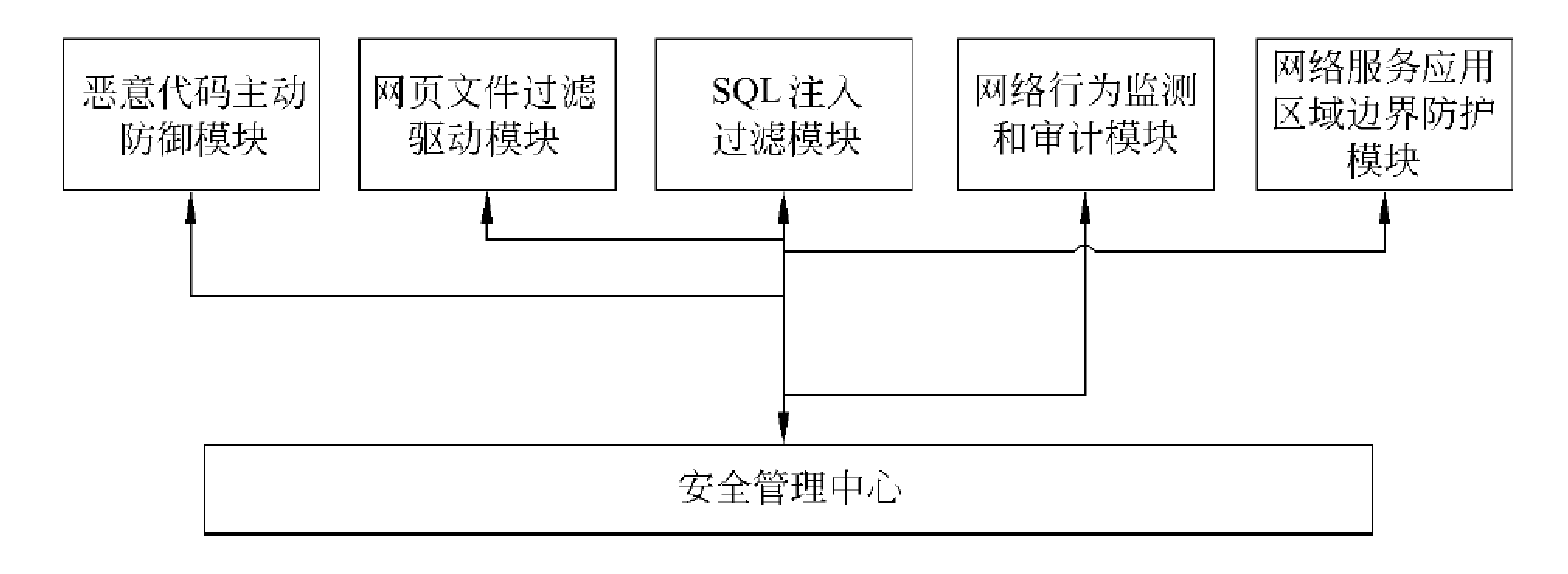



图 4-9　网站防护子系统组成

① 恶意代码主动防御模块：利用信任链机制，对系统中所有装载的可执行文件代码(例如，EXE、DLL、COM 等)进行控制，所有可执行文件代码在加载运行之前都需要先检验，只有通过验证的代码才可以加载。

② 网页文件过滤驱动模块：网站管理员可以自行选择将需要保护的网页文件设定为受控对象，对于每一个受保护的对象，管理员为其设定一个对象相关授权码。对象相关保护方式是一种不基于系统用户身份的访问控制技术，对于所有受保护的对象，网站防护系统在操作系统内核对其加以保护，在不知道对象相关授权码的情况下，即使是系统管理员，系统也禁止其对受保护对象(比如主页)的任何特定操作，比如修改内容、删除、重命名等。通过对象相关保护方式，即使攻击者拿到系统管理员的权限，由于不知道受控对象的授权码，因而也无法对其进行修改，从而可以有效阻止溢出类攻击对系统静态网页的篡改。

③ SQL 注入过滤模块：网站防护系统可以通过高效的 URL 过滤技术，把 SQL 注入的关键字过滤掉，从而有效避免网站服务器受到 SQL 的注入攻击。

④ 网络行为监测和审计模块：在网络传输层面根据等级保护基本要求，从网络层面对网络行为进行监控和审计。

⑤ 网络服务应用区域边界防护模块：阻止传统的非法网络访问，提高网站服务系统的可用性；满足第四级网站系统的结构化要求，从而防止因为这些设备存在安全缺陷导致被内部或外部攻击旁路；实现第四级网站系统和因特网这两个安全域之间的安全隔离；对接入系统的计算平台进行可信验证和接入控制，确保接入系统的平台符合系统安全策略。安全管理中心负责系统安全策略的制定、分发和维护，并集中对系统审计信息进行管理；安全管理策略包括主客体安全级别的定义、系统审计规则、安全管道封装策略等。安全管理中心的另一个功能是对信息进行安全审查，调整信息安全级别，比如，支持低安全级别的信息经过安全审查后，可以提高其安全级别；安全管理中心同样以可信计算平台技术为实现基础。其包含的子系统如以下各节所述。

## 4.8.1　恶意代码主动防御子模块的设计

恶意代码主动防御子模块又分为可执行代码一致性校验和移动代码类验证两个部分。

### 1. 可执行代码一致性校验模块设计

系统服务、系统自启动程序运行后，根据用户的不同需求，需要加载不同的 Windows 应用程序，为防止系统被恶意代码的攻击，需要在操作系统加载运行后对被加载的应用程序(包括.dll 和.exe 等文件)的真实性和完整性进行验证，以确保恶意代码不会被动态装入到系统之中。在对应用程序的真实性和完整性验证方面，本方案采取通过 Hook 实现方法对系统中每一个要加载的可执行代码加以验证，只有符合安全策略的可执行代码才能真正被系统执行。在具体实现上，可以通过对系统函数 Createprocess()和 Loadlibrary()进行 Hook，从而对系统加载和运行的应用程序加以验证，验证过程中的主要验证依据是一个可信程序白名单(Trusted Software List，TSL)，在该名单中列出了系统所有可信的可执行代码文件及其完整性校验值。在系统装载可执行代码之前，应对被加载文件的完整性校验值进行验证，并在 TSL 中查询是否存在对应项目，如果没有，则系统不会加载运行该可执行代码。验证的实现过程如图 4-10 所示。

计算待加载文件的 hash 值
Hook API
该 hash 值在 TSL 中是否有匹配项?
N
Y
Createprocess( )/Loadlibrary( )
Createprocess( )/Loadlibrary( )
记录结果

图 4-10 通过 Hook API 实现应用装载模块验证

在操作系统可信启动的基础上，通过动态多路径信任链(DMPTC)机制，既能保证终端平台的安全可信，又能保证终端平台服务支持和应用选择的灵活性和实用性。DMPTC 验证采用强制型策略机制：所有安全验证策略(即 TSL)由独立的系统安全管理平台制定并分发给各个用户操作终端。图 4-11 给出了 DMPTC 模型的结构图。

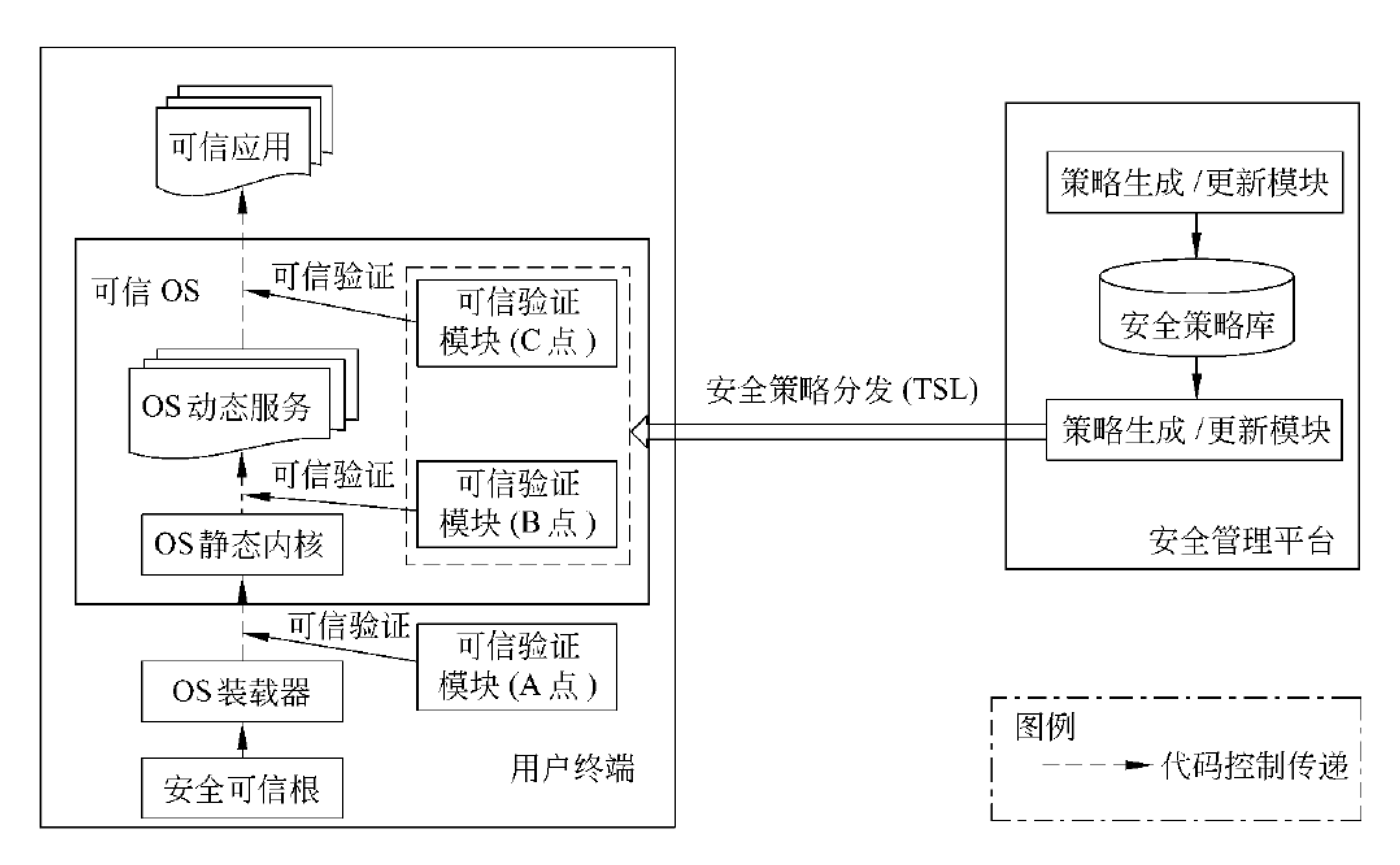



图 4-11 DMPTC 模型结构

在 DMPTC 模型中，TSL 的真实性可以通过安全管理人员的私钥签名机制来保证。

## 2. 移动代码(宏和脚本)类验证模块设计

除了可执行程序的一致性校验工作之外，脚本和宏等解释执行的代码同样需要进行来源和完整性的验证。互联网的飞速发展使人们越来越依赖于网络中的信息，但是，通常情况下这些信息并不是纯数据，而是包含着可执行代码的数据。代码以多种方式混杂在数据中，例如网页中的脚本(script)、文档和电子邮件中的宏(macros)等，这些动态可执行

程序通常被称为移动代码(mobile-code)。移动代码在给使用者带来极大便利的同时，也带来了极大的安全风险。其中，对恶意移动代码(诸如恶意脚本、宏病毒等)的控制一直是业界难以解决的问题。

可以采取以下几种方式对脚本和宏代码实施控制。

(1) 控制独立存在和执行的脚本

Windows 的 WSH 服务负责解释和执行以 VBS 和 JS 为后缀的脚本文件，通过在 WSH 服务的两个进程(Wscript. exe 和 Cscript. exe)中增加安全验证模块，使其能够在执行前对脚本的数字签名进行验证，从而只允许具有管理中心合法签名的脚本获得执行。

为了对合法脚本文件进行标识，本方案在管理中心增加数字签名模块，在合法的脚本文件中增加管理中心的数字签名，将签名以注释形式存放于脚本代码中，增加的签名不影响脚本原有代码的正常执行。

这种方式控制的对象是以独立文件形式存在于系统的脚本中，由于这类脚本并不内嵌于网页和应用文档中，没有跨平台特征，因此能够有效避免恶意脚本的攻击。

(2) 控制 Office 中的宏

Office 软件已经具有对脚本和宏的安全限制，Office XP 应用程序宏安全性的选项如下所述。

① 高：只允许运行来源可靠的签名宏，自动禁用未签名的宏。

② 中：可以选择是否运行潜在不安全的宏。当打开包含宏的文档时，就会要求确认是否运行这些宏。

③ 低：运行所有的宏，而不给出任何安全警告。

Office 原有机制对以上安全级别设置是自主型的，本方案将其安全级别固定为高级别，之后不允许任何进程修改其安全级别，这样一来，具有可靠来源数字签名的宏就会被允许执行，没有数字签名的宏将被禁止执行，而其他具有数字签名的宏在执行前，系统将对用户进行提示以决定是否执行，如图 4-12 所示。

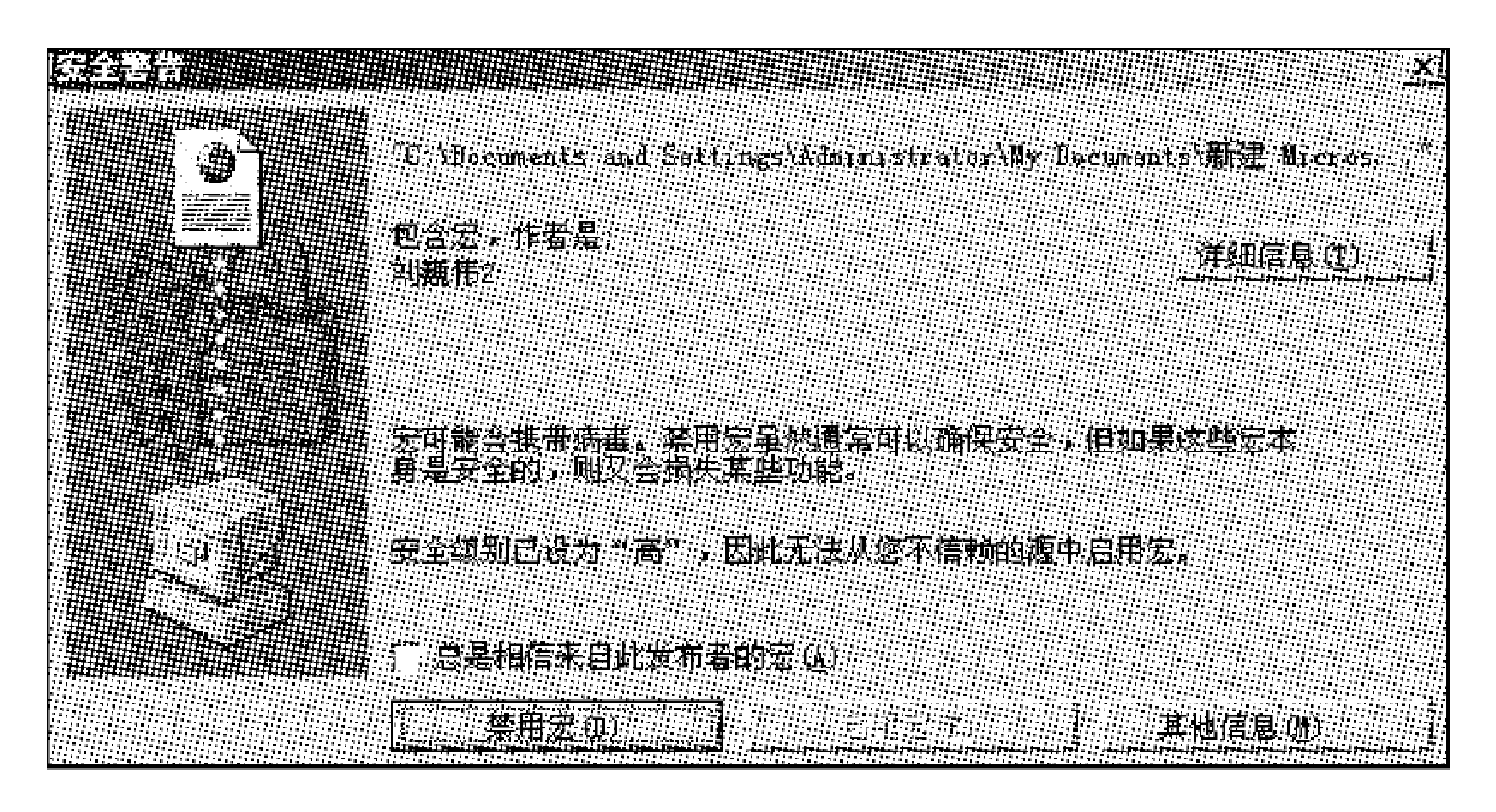



图 4-12　系统将对用户进行提示

### 4.8.2 网页文件过滤驱动保护子模块的设计

Windows 系统是一种自主型访问控制系统，这类系统主要服务于个人系统。但是，在政府和企业等生产型系统中，自主型访问控制机制不能适应这类应用系统的组织和业务结构，难以完全满足业务应用对多级安全访问控制的安全需求。

自主型访问控制系统的另一个安全局限性表现为其难以阻止溢出类黑客攻击。溢出类黑客攻击是目前最主要的，也是危害性最大的安全攻击类型之一。溢出类攻击中，黑客可以通过系统漏洞获取系统管理员权限。目前，Windows 的安全机制无法识别并阻止黑客的这类攻击行为。在 Windows 的安全增强设计方案中，我们提出了一种与用户身份无关的访问控制机制——对象相关(Object-Specific)访问控制机制，它是一种不基于用户身份的访问控制机制，可以对系统或应用的重要数据和资源进行保护，即使是系统管理员，只要没有授权，也无法访问特定的对象。

对象相关访问控制主要是针对利用溢出类的黑客攻击。对象相关保护方式是一种不基于访问用户身份的访问控制技术，它运行在系统内核。对于每一个受保护的对象，对象所有者为其设定一个对象相关授权码，在不知道对象相关授权码的情况下，即使是系统管理员，系统也禁止其对于受保护对象(比如主页)的任何特定操作，例如修改内容、删除、重命名等。

由于对象相关的数据保护与访问用户身份无关，因此，通过对象相关的数据保护方式可以有效阻止溢出类攻击对系统重要文件和用户重要数据的窃取和篡改。例如，Web 防篡改保护，对网页数据以及 Web 服务(例如，IIS、APACHE)的相关配置文件也采用此方式进行保护，以防止通过修改配置文件达到篡改网页的目的。

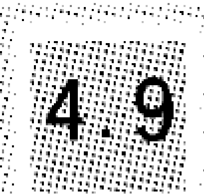
虽然对象相关访问控制不能消除基于系统漏洞的攻击，但是，它可以减少黑客攻击给系统带来的危害程度。

### 4.8.3 网站服务应用区域边界防护

网站服务应用区域边界措施包括可信防火墙和可信网站安全服务网关。其中，防火墙可以有效减少进入系统的网络流量，除了阻止传统的非法网络访问外，它还可以提高网站服务系统的可用性。可信防火墙和可信网站安全服务网关要基于可信计算平台技术来实现，满足第四级网站系统的结构化要求，从而防止因为这些设备存在安全缺陷而导致被内部或外部攻击旁路。可信网站安全服务网关的另一个作用是实现第四级网站系统和因特网这两个安全域之间的安全隔离。应用区域边界的另一个安全措施建议是对接入系统的计算平台进行可信验证和接入控制，确保接入系统的平台符合系统的安全策略。

网络接入控制可以通过平台可信证明机制来实现，保证接入系统的各个计算平台在安全策略上保持一致，比如对安全标记解释的一致性、对安全策略执行的一致性等。在本方案中，建议将系统安全策略作为平台可信度量和验证的一个基础性指标。

可信网站安全服务网关是针对网站服务系统安全特性的应用区域边界措施，是另一种类型的安全管道封装技术，包括动网信息的安全性。网关对用户提交信息进行安全审查，防止 SQL 注入和跨站类攻击的发生；同时还对 DDOS/DOS 攻击有抵制功能。



# 4.9 示范环境功能使用操作演示

## 1. 发行用户硬件令牌

发 KEY 操作只能在安全管理平台所在的机器上进行，如图 4-13 所示。

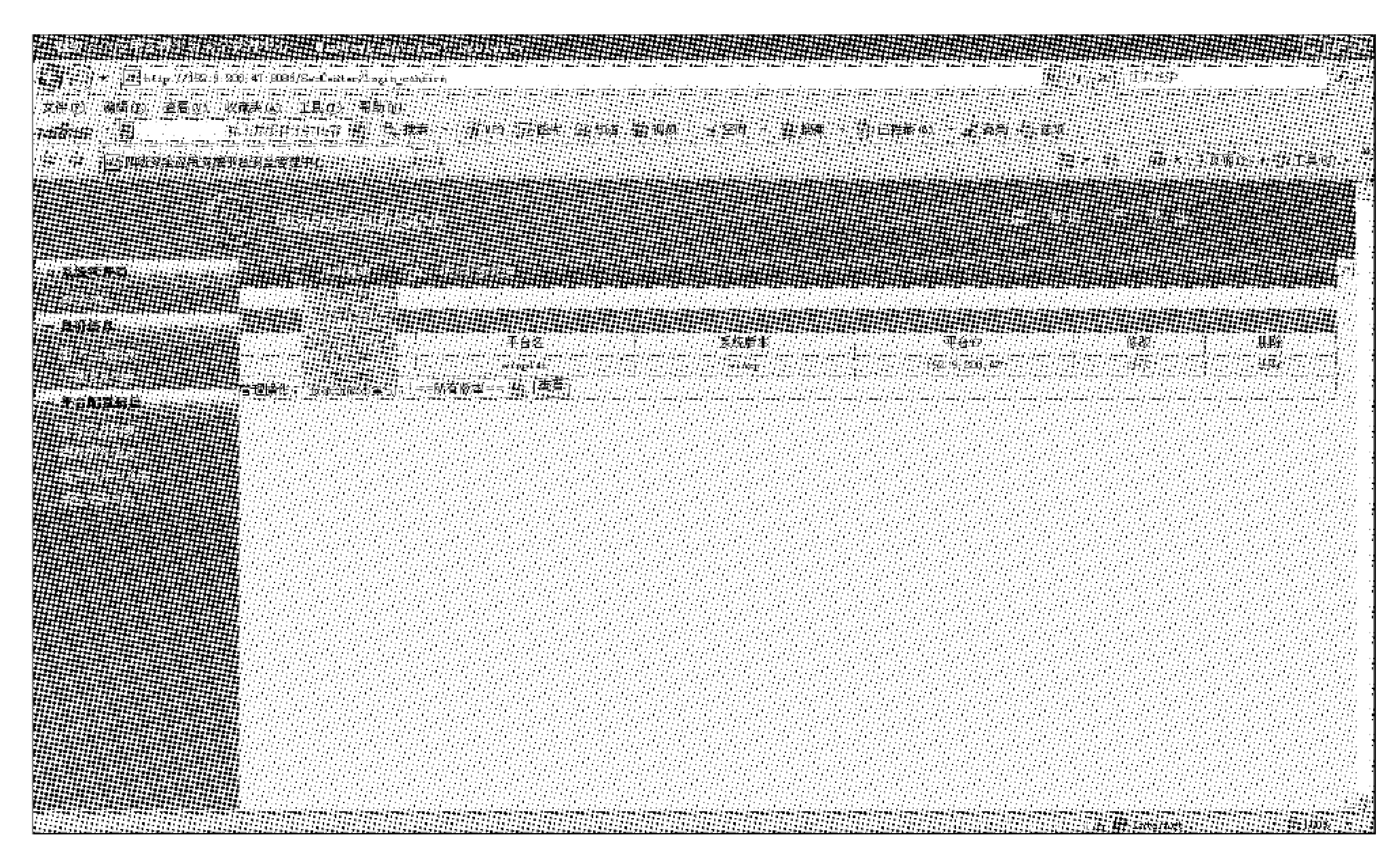


图 4-13　发 KEY 操作界面

## 2. 安全管理员制定策略

单击左边操作栏“策略管理”下的“范畴管理”选项，进入范畴管理主界面制定策略，如图 4-14 所示。

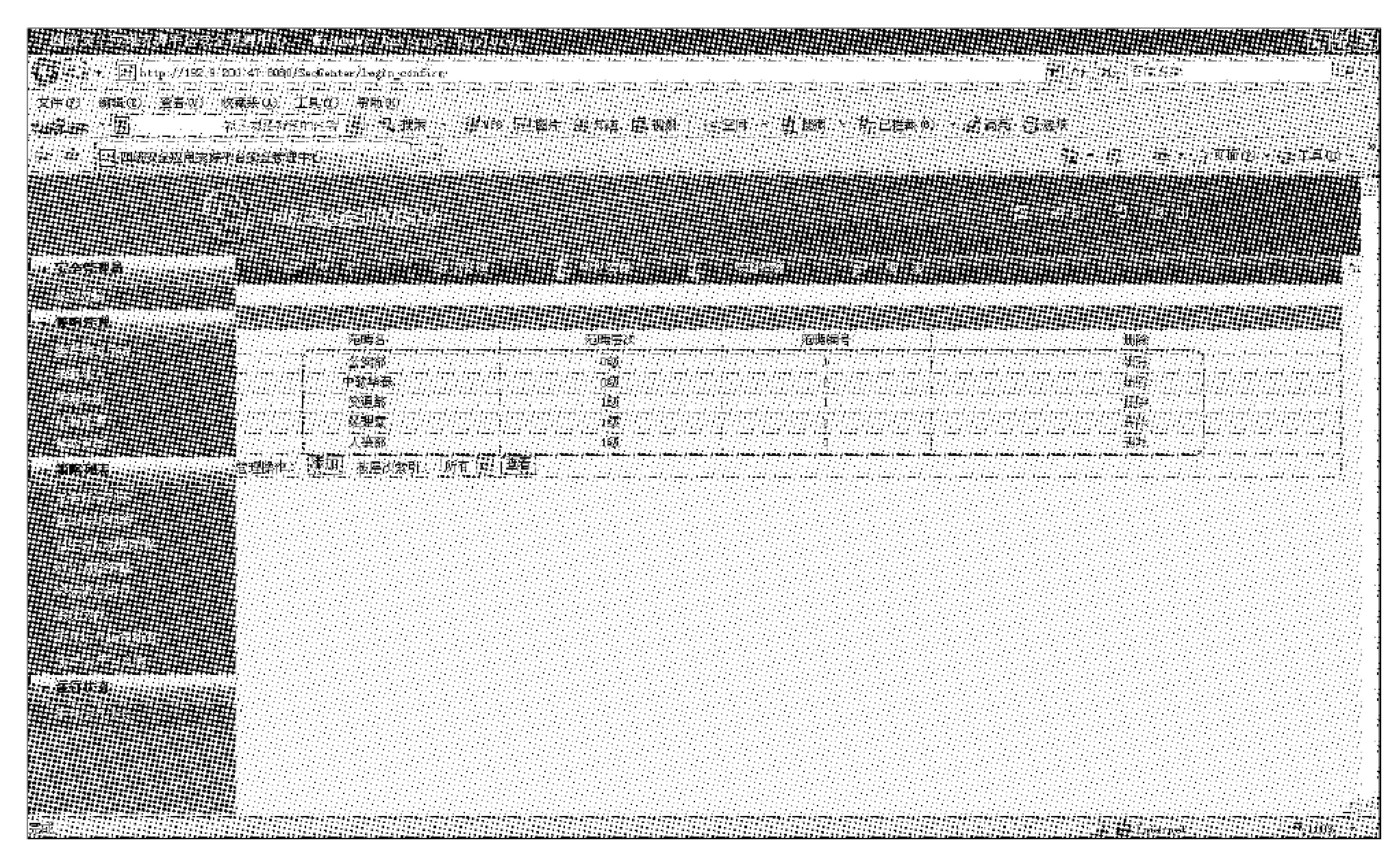


图 4-14　安全管理员制定策略界面

### 3. 安全管理员可执行代码预期值授权

安全管理员将可执行程序列表中的合法程序执行权限授予相应的用户，如图 4-15 所示。

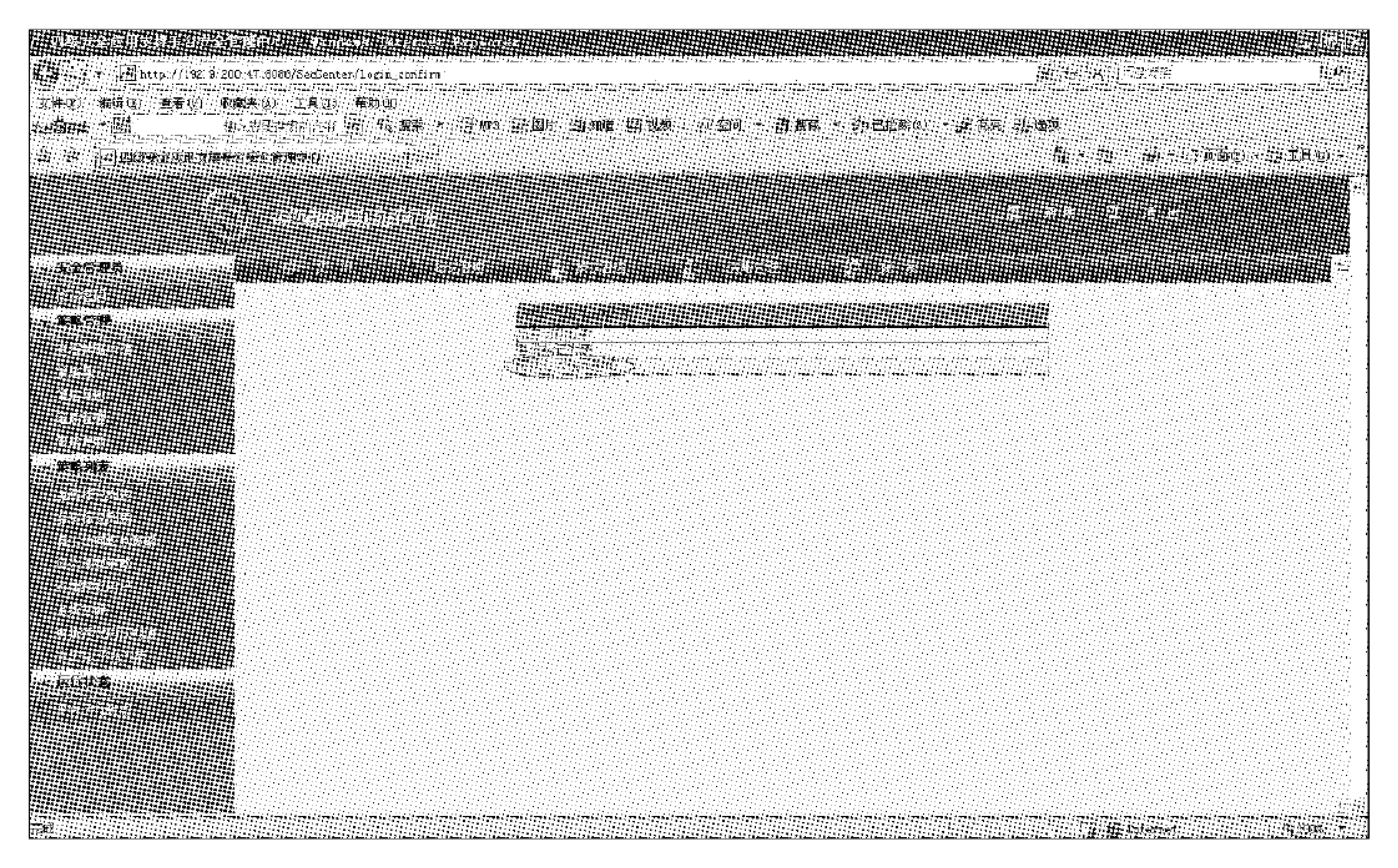


图 4-15 安全管理员可执行代码预期值授权界面

### 4. 设置平台状态

进入平台运行状态主界面设置平台状态，如图 4-16 所示。

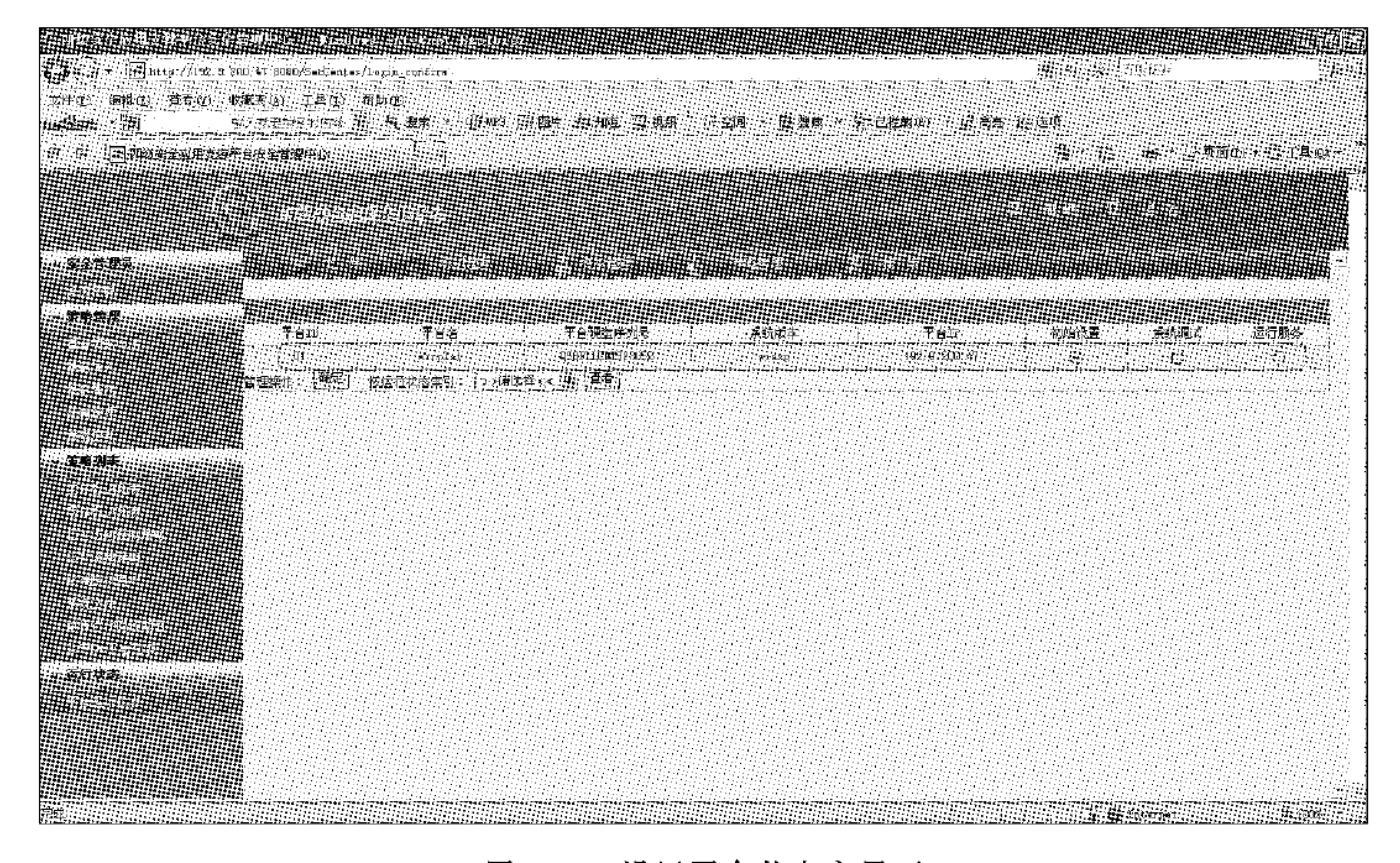


图 4-16 设置平台状态主界面

## 5. 审计管理操作

安全审计员正常登录系统，进入审计管理主界面进行审计，如图 4-17 所示。

图 4-17　审计管理操作主界面

## 6. 强制访问控制策略授权

将文件访问操作权限授予相应用户，加入强制访问控制列表，如图 4-18 所示。

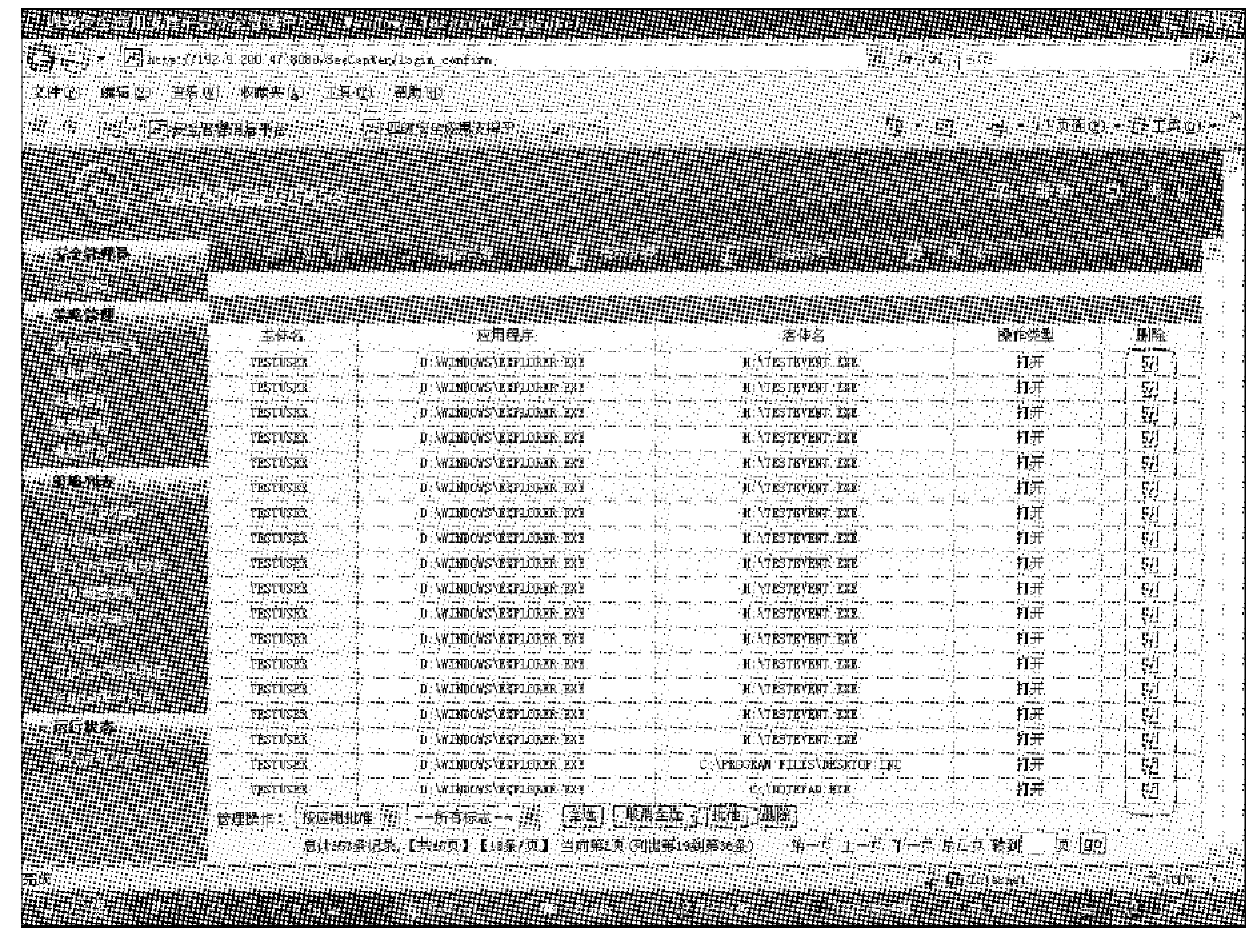


图 4-18　强制访问控制策略授权界面

# 第5章 二、三、四级安全应用平台功能符合性检验工具集的使用

## 5.1 总体结构

安全功能符合性检验工具集的目的是针对安全应用平台进行功能的审核和检验。安全应用平台分别从安全计算环境、安全区域边界、安全通信网络和安全管理中心四个方面进行搭建，安全功能符合性检验工具集针对四个方面的功能点进行审核检验。可以说安全功能符合性检验工具集是一个针对信息系统安全功能的检验，各个安全功能具体由功能点和功能要素得到体现。

安全功能符合性检验工具集若要完成如上提出的功能检验，不可或缺的部分就是信息系统检验功能的分界。这一映射功能在考虑功能的同时，更应该紧紧围绕 GB 17859—1999 的功能规定，借助功能要素完成功能映射。同时为了达到 GB 17859—1999 规定的功能要求，在映射过程中应参考等级保护相关标准完成系统扩展功能的功能要素映射。可见，安全功能符合性检验工具集依据 GB 17859—1999，同时融合其他相关标准，具备信息系统到安全功能映射的一个检验工具集，是一个既可以对信息系统安全功能，又可以对特定安全功能进行检验的工具集。

安全功能符合性检验工具集的总体结构如图 5-1 所示。检验工具集针对各个功能的检验通过三个子模块来完成，分别是：数据获取子模块、数据分析（检验）子模块和数据处理子模块。其中数据获取部分可以通过网络数据获取或本地数据获取的方式收集安全应用平台中各子系统的交互数据；数据分析则在数据获取的基础上，与人工检查的方式相结合，通过半自动化的方式对各个检验项的符合性进行检验，重点是数据分析的方法和流程；数据处理则是对获取的数据和检验结果的存储，重点是解决数据获取与数据分析之间的数据交互以及数据分析结果的处理问题。

图 5-1 安全功能符合性检验工具集结构

## 5.2 功能结构

安全功能符合性检验工具集总体功能结构如图 5-2 所示。检验工具集共包含数据获取、数据导入、项目管理、手工检查、数据分析、结果处理和设计要求检验策略库管理七个模块。

数据获取模块负责从目标系统捕获检验过程中所需要的各种业务数据。主要包含数据监听和导出数据解析两个模块。数据监听模块通过接收用户设定的监听参数捕获网络中的数据包，经过协议过滤和解析后对数据进行保存。导出数据解析模块根据不同类型的二进制数据，按照应用平台设计要求中所定义的数据结构，将其解析为检验工具集内部所能识别的数据结构。

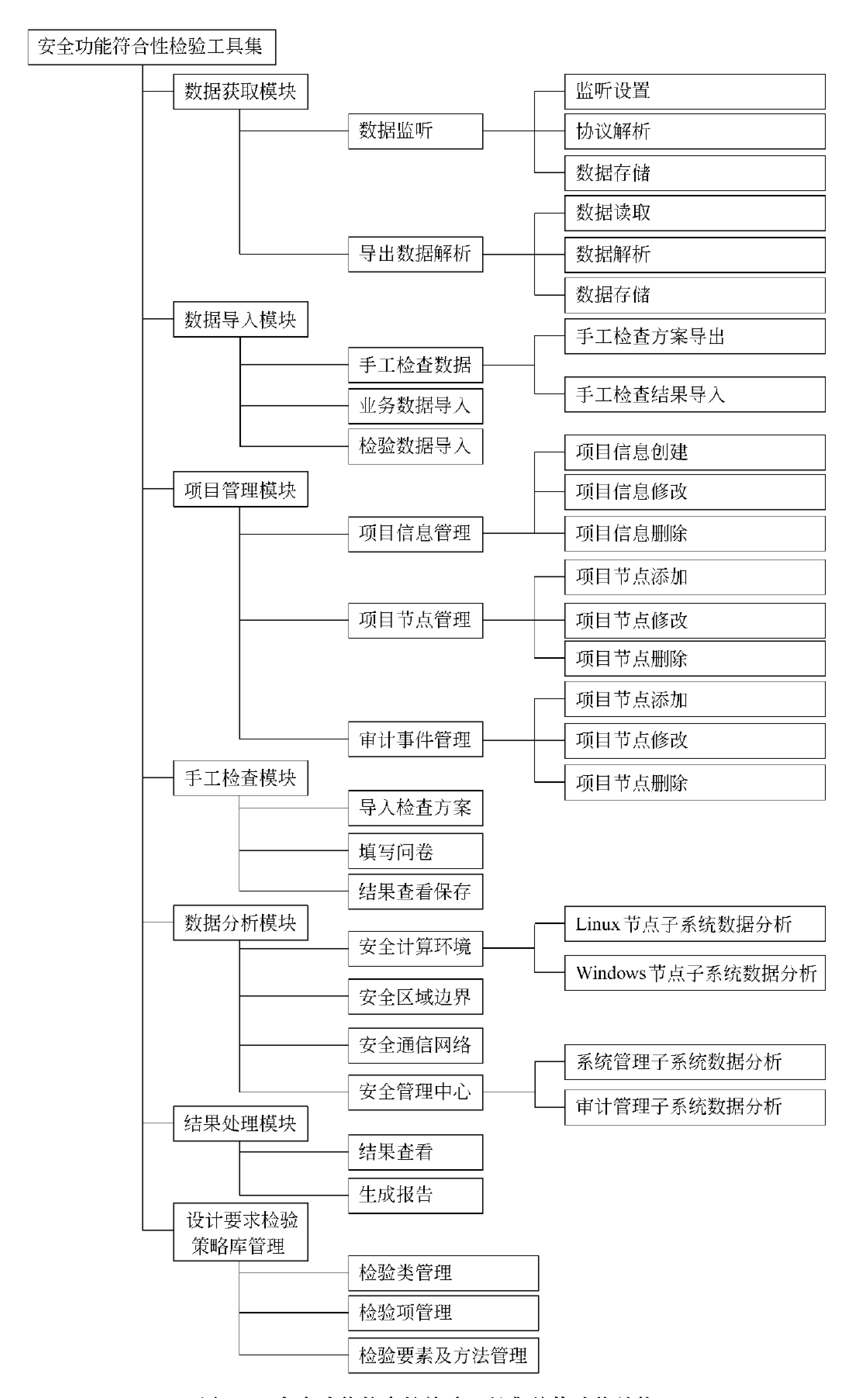



图 5-2 安全功能符合性检验工具集总体功能结构

数据导入模块是各个功能子模块进行数据交互的接口，主要包含手工检查方案导出、手工检验结果导入、检验数据导入和业务数据导入四个子功能。检验数据导入功能负责在检验开始前将设计要求检验策略库中的检验数据导入到项目数据库中，以便操作员根据需要对检验要素进行取舍。业务数据导入功能负责将数据获取模块生成的 XML 格式的业务数据导入到项目数据库中，以便检验工具集的数据分析模块来调用分析。

项目管理模块用于检验工具集检验项目的初始化工作。包含项目信息管理、项目节点管理以及事件类型管理三个子模块。项目信息管理负责添加、修改以及删除项目信息，并对项目信息指定负责人以及设定是否为当前检验项目。项目节点管理主要功能是管理当前项目所拥有的节点信息，包含计算环境及其子节点信息、区域边界节点信息、通信网络节点信息以及管理中心及其子节点信息。事件类型管理主要功能是导入安全应用平台设计实现时所定义的各种安全设计事件，并将这些审计事件与检验工具集内部所定义的事件类型进行关联对应。

手工检查模块完成手工检验要素的检验。通过导入当前项目的手工检查方案，调用各个检验要素的检验方法和检验流程，指导操作人员完成手工检验，并将检验结果保存到手工检查方案中。

数据分析模块的主要功能是调用数据获取端捕获的各种业务数据，依据特定的算法对各个检验要素进行功能符合性检验。主要包含计算环境、区域边界、通信网络以及管理中心数据分析。

结果处理模块的主要功能是对数据分析模块输出的数据进行统计分析，生成相应的统计图，并对检验项目出具详细的检验报告。

设计要求检验策略库管理模块负责对设计要求检验策略库进行数据维护。主要包含检验项管理、检验类管理、检验要素以及方法管理。

## 5.3　设计与实现

### 5.3.1　数据获取模块

#### 1. 功能概述

数据获取模块位于目标系统内部，以旁路的方式监听安全应用平台各个子系统之间的通信数据。数据获取模块是进行数据采集和解析的必要部件，也是进行数据分析的前提。数据获取模块的主要功能是实时监听、解析网络流量数据包，并且解析目标系统导出的业务数据。

#### 2. 设计结构

数据获取模块为检验工具集提供一个与目标系统进行数据交互的接口，作为一个单独的模块运行在目标系统内部，与各个节点子系统进行旁路连接。数据获取模块的功能主要分为系统管理、监听设置、网络数据监听和数据解析四个部分。其中数据解析包含监

听数据解析和导出数据解析两个子模块。具体功能结构如图 5-3 所示。

(1) 系统管理

数据获取模块作为一个独立运行的模块，拥有自己的图形用户界面，因此需要为用户提供一个简单的系统管理功能，包括系统的启动、退出等。

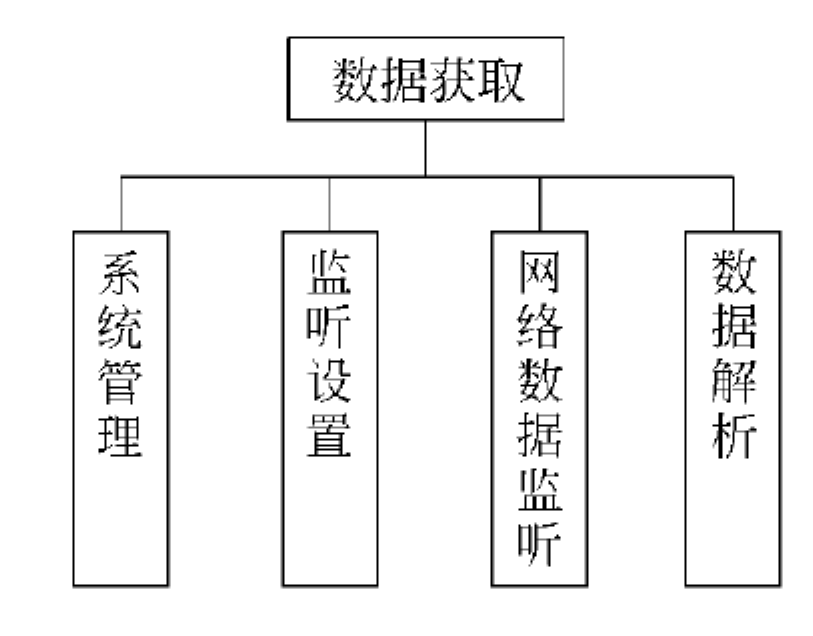



图 5-3 数据获取模块的功能结构

(2) 监听设置

监听设置负责设置网络监听时系统需要用户选择或提供的各种参数。包括监听数据时所需的网卡名称，数据获取模块当前所部署的节点位置等信息。

(3) 网络数据监听

网络数据监听是数据获取模块需要完成的主要功能。数据获取模块通过调用 winpcap 底层驱动程序，捕获所有流经当前网卡的数据包。并将捕获的数据包信息及时显示在用户界面中。当用户触发停止监听请求后，数据获取模块自动将捕获的数据包信息存储在本地文件中。

(4) 数据解析

数据解析包含监听数据解析和导出数据解析两部分内容。

① 监听数据解析

数据获取模块在进行网络监听时会对所捕获的数据包进行实时解析，根据数据包封装协议的不同对数据包进行适当过滤，将检验工具集所需要的数据包重新封装成工具集内部的数据结构，并存储为统一格式的接口文件。

② 导出数据解析

检验工具集所需要的部分业务数据需要以管理员的身份从目标节点子系统导出。而这部分导出数据都是以二进制的格式进行存储，不能直接应用于检验工具集进行数据分析，因此需要对其进行进一步的解析，使其符合检验工具集内部的数据结构。导出数据解析根据不同的数据类型又可以分为自主访问控制列表数据解析、审计策略列表数据解析以及审计信息数据解析等。

## 5.3.2 数据导入模块

### 1. 功能概述

数据导入模块是数据获取模块、检验工具集、设计要求检验策略库以及手工检查工具之间的接口。

数据获取模块作为一个单独的应用程序与安全应用平台网络内部的节点子系统进行旁路连接，其捕获的业务数据经过解析保存后需要通过数据导入模块导入到检验工具集，供数据分析模块分析处理。

设计要求检验策略库用于存储检验工具集的检验内容和检验方法，是检验工具集对安全应用平台各个节点子系统进行功能符合性检验的标准和依据。检验开始前需要将设计要求检验策略库中的检验内容通过数据导入模块导入到项目数据库中，由操作员在检验过程中根据实际情况对检验内容进行过滤取舍。

手工检查工具作为一个单独模块，调用检验工具集导出的手工检查方案为操作人员在手工检验过程中提供向导和指南，并将手工检验结果通过数据导入模块反馈给检验工具集。

## 2. 设计结构

数据导入模块共包含四个功能：手工检查方案导出、手工检查结果导入、业务数据导入以及检验数据导入。数据导入模块的主要功能结构如图 5-4 所示。

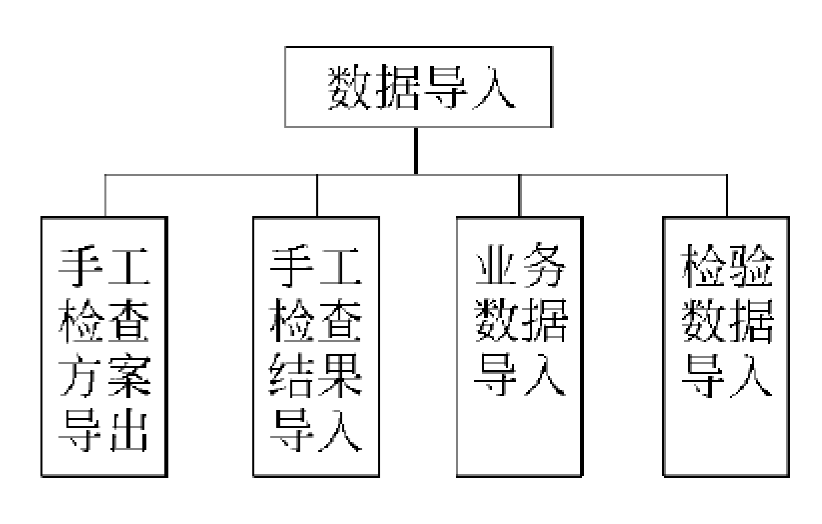



图 5-4　数据导入模块功能结构

① 手工检查方案导出：将当前检验项目中的手工检验要素信息，以及相应的检验流程和检验方法导出成 XML 格式文件。

② 手工检查结果导入：将手工检查工具生成的检验结果导入到项目数据库中，便于数据分析模块以及结果处理模块进行数据分析。

③ 业务数据导入：将数据获取模块捕获的各种业务数据导入到项目数据库中，作为对检验要素进行功能符合性检验的依据。

④ 检验数据导入：与设计要求检验策略库相关，负责把当前项目的检验数据从设计要求检验策略库中导入到项目数据库。

# 5.3.3　项目管理模块

## 1. 功能概述

项目管理模块是检验工具集进行功能符合性检验的前提，负责对被检验项目中的项目信息、项目节点及项目检验中所需审计事件等进行配置管理，是对被检验项目的一个初始化和后续配置的过程。项目管理模块包括项目信息管理、项目节点管理和审计事件管理三个子模块。

## 2. 设计结构

项目管理模块的功能结构，如图 5-5 所示。

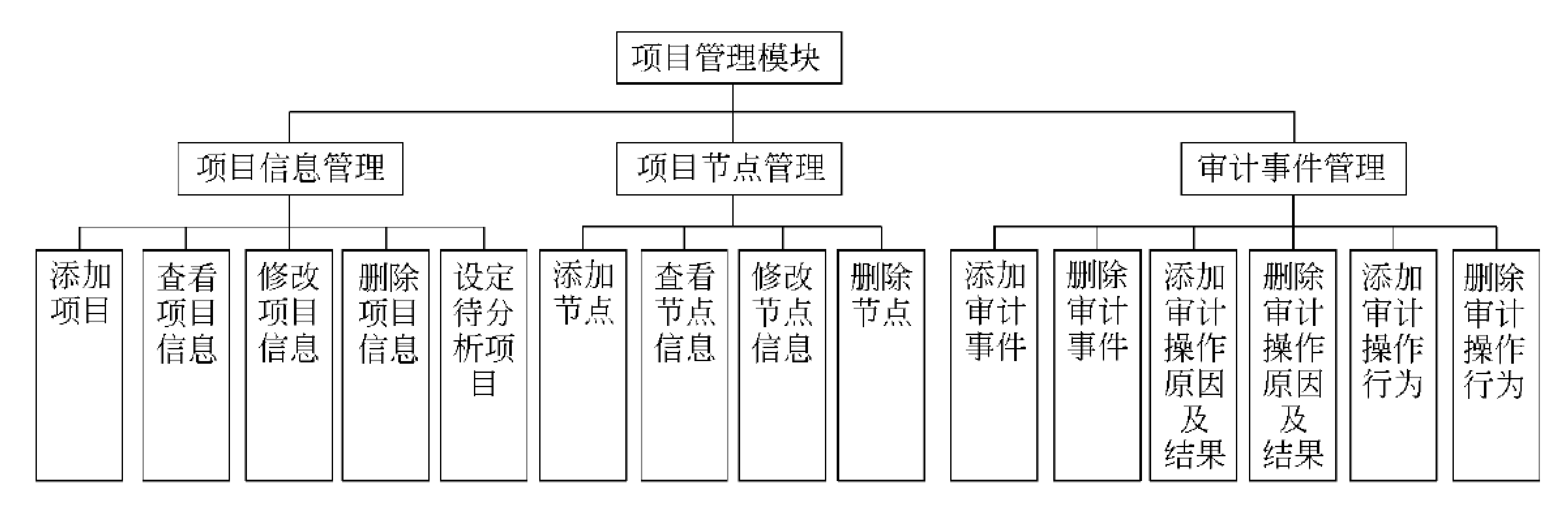



图 5-5　项目管理模块功能结构

(1) 项目信息管理

项目信息的管理包括：添加项目、查看项目信息、修改项目信息、删除项目信息和设定待分析项目。

① 添加项目：添加新的检验项目。添加的信息包括项目编号、项目等级、项目名称、创建时间、负责人委托单位、检测单位、整体描述和项目的备注等。

② 查看项目信息：查看某一检验项目的信息，包括项目编号、项目名称、项目等级、创建时间、完成时间、负责人、委托单位、检测单位、项目状态、检验结果、项目描述以及项目备注等信息。

③ 修改项目信息：修改某一检验项目的信息，包括项目编号、项目等级、项目名称、委托单位、检测单位、负责人、检验结果、项目状态、结束时间、项目整体描述以及项目备注等信息。

④ 删除项目信息：删除某一检验项目，同时删除与该项目相关的所有信息，包括该项目的节点、检验数据以及项目的审计事件等。

⑤ 设定待分析项目：将某一检验项目设定为即将进行数据分析的当前项目。

(2) 项目节点管理

项目节点管理包括：添加节点、查看节点信息、修改节点信息和删除节点。

① 添加节点：添加新的项目节点。添加的信息包括节点编号、节点标志、节点所属系统类型、节点 IP 地址、节点 MAC 地址、节点描述以及节点的各个检验项和各个检验要素信息等。

② 查看节点信息：查看某一节点的详细信息，包括节点编号、节点标志、节点所属系统类型、节点 IP 地址、节点 MAC 地址和节点描述等信息。

③ 修改节点信息：修改某一节点的信息，包括节点编号、节点标志、节点所属系统类型、节点 IP 地址、节点 MAC 地址和节点描述等信息。

④ 删除节点：删除某一节点，同时删除与该节点相关的所有信息，包括该节点的检验项和检验要素等信息。

(3) 项目的审计事件管理

项目的审计事件管理包括添加审计事件、删除审计事件、添加审计操作原因及结果、删除审计操作原因及结果、添加审计操作行为和删除审计操作行为。

① 添加审计事件：根据当前检验项目的需要，为当前被检验项目添加审计事件。

② 删除审计事件：删除当前被检验项目中的某些审计事件。

③ 添加审计操作原因及结果：若现有的审计事件中的审计操作原因及结果不能满足当前项目的要求时，添加审计事件中的操作原因及结果。

④ 删除审计操作原因及结果：删除审计事件中的某些操作原因及结果。

⑤ 添加审计操作行为：若现有的审计事件中的审计操作行为不能满足当前项目的要求时，添加审计事件中的审计操作行为。

⑥ 删除审计操作行为：删除审计事件中的某些操作行为。

### 5.3.4 手工检查工具模块

#### 1. 功能概述

"手工检查工具"是等级保护检验工具集的一部分，通过"手工检查工具"可以辅助用户利用检验工具集对等级保护安全平台进行检验时，采用向导的方式对不能自动和半自动检验的检验要素进行手工检验。

#### 2. 设计结构

"手工检查工具"分为三个模块，分别是数据导入、问卷调查和结果查看。首先应该在检查之前导入数据，数据源是 XML 文件，此时需要检查的数据就会在界面上显示出来，用户根据提示，对每一个检验要素进行检验，并填写调查问卷，填写后的内容将被写入到 XML 文件当中，最后可以查看检验结果。

(1) 数据导入

数据导入模块主要实现手工检验数据的导入，数据源是 XML 文件。当载入文件路径时，通过相关 XSD 文件判定该文件格式是否符合要求，如果符合则导入数据，为下一步调查问卷的生成做好准备。

(2) 问卷调查

问卷调查模块主要实现引导用户对等级保护安全平台做手工检查，并将检查结果回填到 XML 文件中，以便将 XML 文件导入到数据分析系统进行综合处理。

(3) 结果查看

结果查看模块主要实现的是用户检查完毕后，通过界面可以查看每一个检验要素的检查结果，其中包括该要素检验合格与否，以及相关检验记录。

### 5.3.5 数据分析模块

#### 1. 功能概述

数据分析模块是安全功能符合性检验工具集的核心，负责对安全应用平台各个节点子系统进行功能符合性检验。安全应用平台包含七个节点子系统，每个节点子系统都需要实现特定的功能。为此，在数据分析过程中，我们将节点子系统实现的功能点作为检验项，每个检验项划分为更加精确的检验要素。在实际检验过程中，数据分析的检验粒度为检验要素，只要隶属于检验项的所有检验要素都通过功能符合性检验，则认为该检验项合格。如果隶属于节点子系统的所有检验项都满足功能符合性检验，则该节点子系统合格。

检验要素分为自动、半自动和手工三种检验方式。其中手工检查方式的检验要素由手工检查模块完成相应检验。数据分析模块主要针对自动和半自动方式的检验要素进行检验。

在检验过程中，针对每一个自动方式的检验要素都会为其匹配一个检验方法，自动完成功能符合性检验。对于半自动方式的检验要素，需要向用户提供一个交互界面，指导用户根据一定的操作流程判断当前检验要素是否合格。

当用户触发"开始分析"请求后，首先判断"手工检查"的结果是否已经导入，如果没有

给出提示则由用户选择是否继续后续检验，然后检查半自动检验和自动检验所需的数据是否准备好，如果没有给出提示，在文本进度框中显示不齐全的数据列表，则由用户选择是否继续后续检验。如果继续，则循环遍历每个检验项中的检验要素列表，针对每个自动和半自动检验要素调用相应的算法完成功能符合性检验。

## 2. 设计结构

数据分析模块主要完成对安全应用平台各个节点子系统的功能符合性检验。包括安全计算环境数据分析、安全区域边界数据分析、安全通信网络数据分析以及安全管理中心数据分析四个功能模块，如图 5-6 所示。

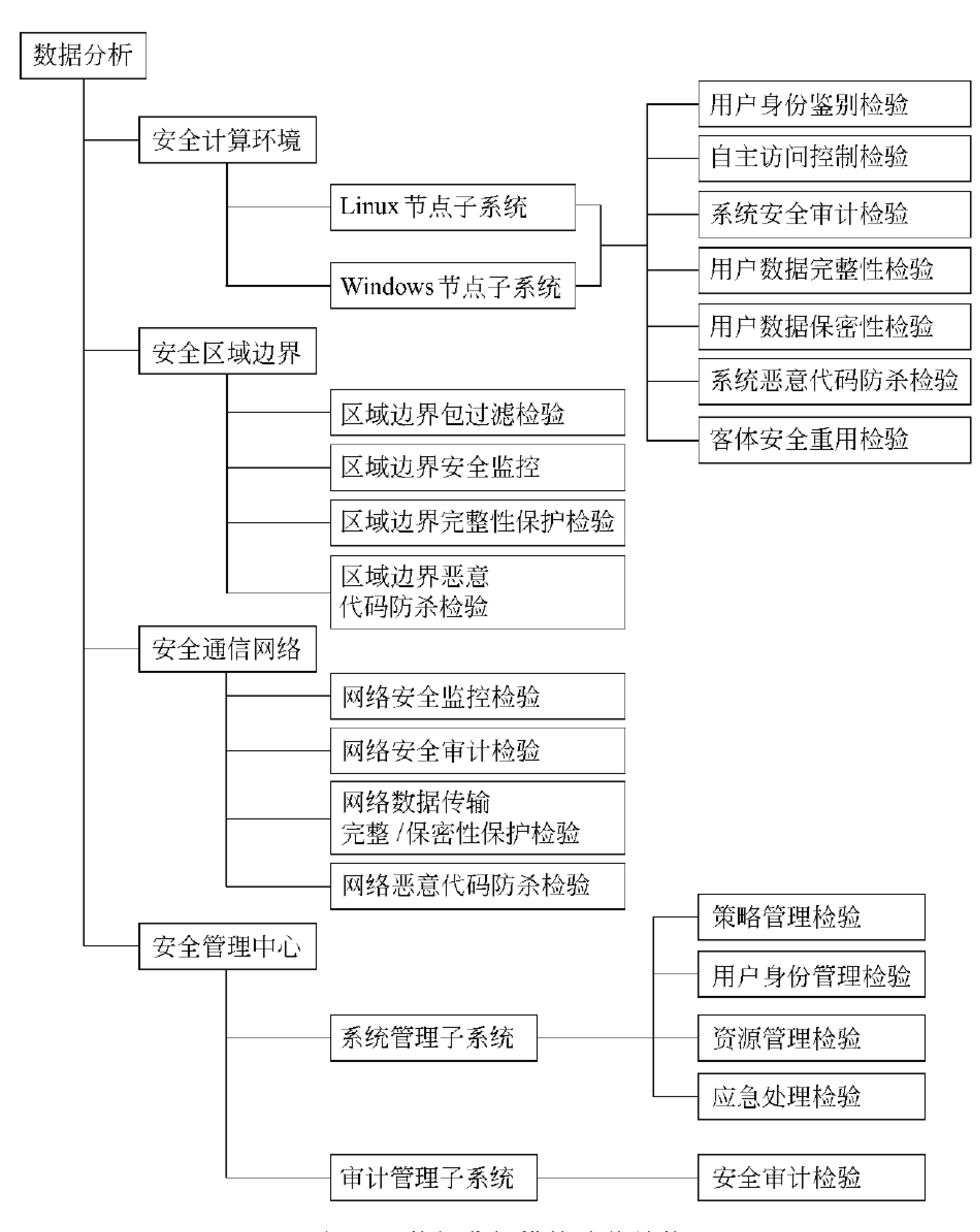



图 5-6 数据分析模块功能结构

(1) 安全计算环境数据分析

安全计算环境数据分析分为 Linux 节点子系统数据分析和 Windows 节点子系统数据分析。由于两个子系统都属于安全操作系统，因此拥有共同的检验项和检验要素，但在

实际检验过程中，不同的操作系统对数据的存储和管理模式各不相同，因此业务数据和检验结果也会发生变化。

(2) 安全区域边界数据分析

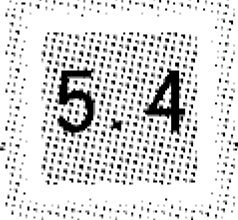
安全区域边界数据分析主要完成对区域边界包过滤、区域边界安全监控、区域边界完整性保护以及区域边界恶意代码防杀检验。

(3) 安全通信网络数据分析

安全通信网络数据分析主要完成对网络安全监控、网络安全审计、网络数据传输完整/保密性保护以及网络恶意代码防杀检验。

(4) 安全管理中心数据分析

安全管理中心数据分析包含对系统管理子系统和审计管理子系统的功能符合性检验。



# 5.4 使用操作演示

## 5.4.1 数据获取端

数据获取工具的网络监听功能包含监听参数设置和数据包监听两部分，与数据解析功能一起构成数据获取工具。

### 1. 监听设置

监听设置功能是完成网络监听前必要的参数设置，包含数据获取平台在安全应用平台网络内部的部署位置，以及用于数据包监听的网卡序号。

在主界面中单击“启动监听”按钮就可以进入“监听参数设置”，如图 5-7 所示。

在“监听参数设置”界面中单击“获取网卡列表”按钮后，在“本机网卡列表”中会依次罗列出本机上所有网卡的编号和描述信息，操作员在文本框中输入需要进行监听的网卡编号后，单击“确定”按钮即可开始网络数据包监听，如图 5-7 所示。

图 5-7　监听参数设置

### 2. 数据包监听

设置完监听参数后，系统将自动进入数据包监听状态。监听过程如图 5-8 所示。监听完成后，单击“ ”按钮，系统将自动保存监听到的数据包。

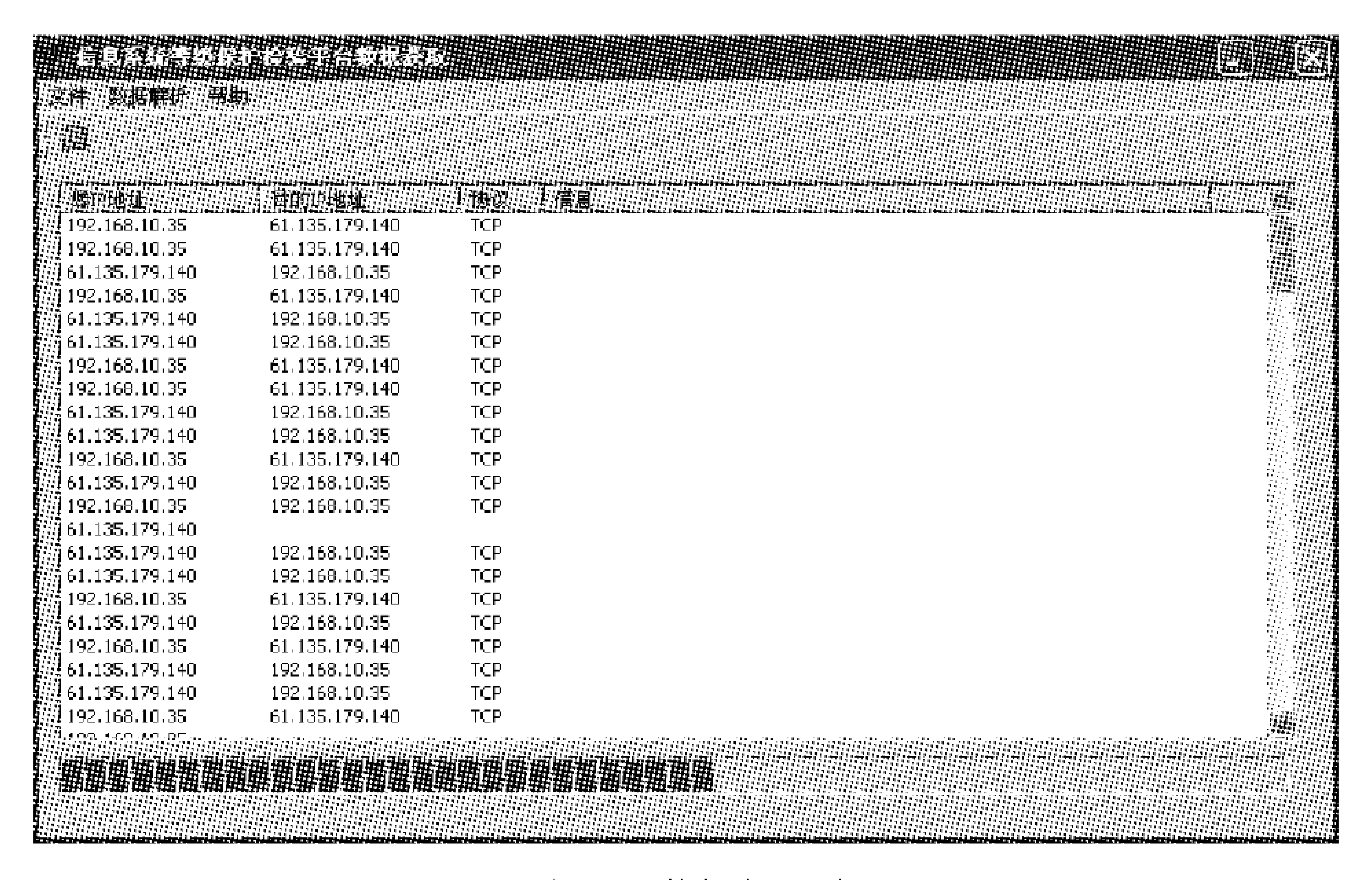



图 5-8 数据包监听

### 3. 数据解析

在主界面中单击“导出数据解析”菜单，进入数据解析界面，如图 5-9 所示。在弹出的“信息系统等级保护检验平台数据解析”界面中，选择需要解析的数据类型以及与之相对应的文件存储路径，单击“确定”按钮即完成当前数据类型的数据解析。

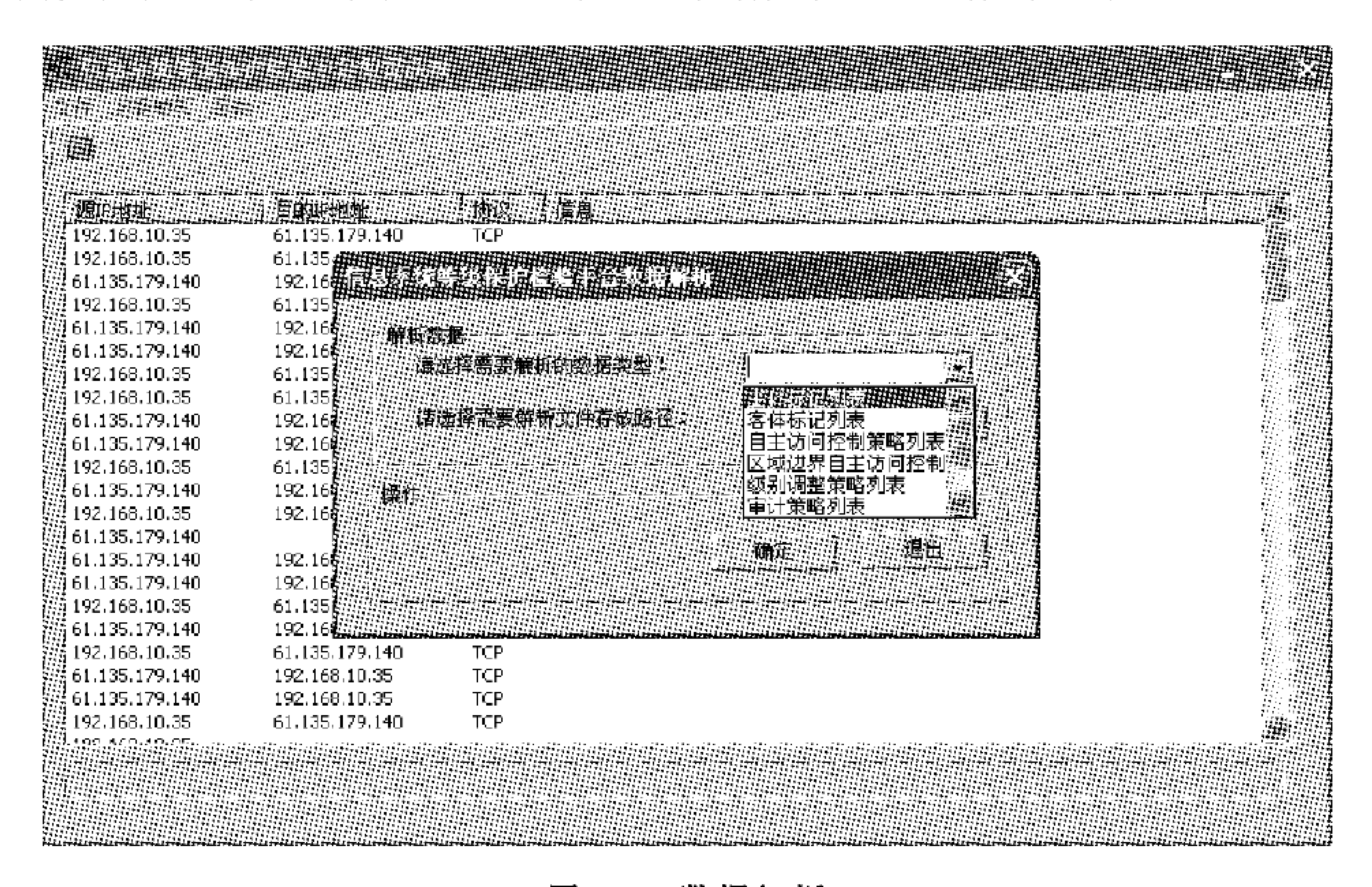



图 5-9 数据解析

## 5.4.2 数据分析端

检验工具集数据分析端分为系统管理员功能模块和普通用户功能模块。

### 1. 系统管理员功能模块

以系统管理员身份登录系统后，可以看到系统主要包括用户管理和项目信息管理等功能。

(1) 用户管理

① 全部用户管理

“全部用户管理”包括用户的添加、修改、删除和退出等功能。

单击“用户管理”|“全部用户管理”菜单或单击快捷工具栏上的“ ”图标，系统将弹出“用户管理”对话框。在对话框中可以看到用户管理包含用户信息的添加、修改和删除的操作。

• 添加用户

单击“添加”按钮，将弹出“添加用户”对话框，如图 5-10 所示。

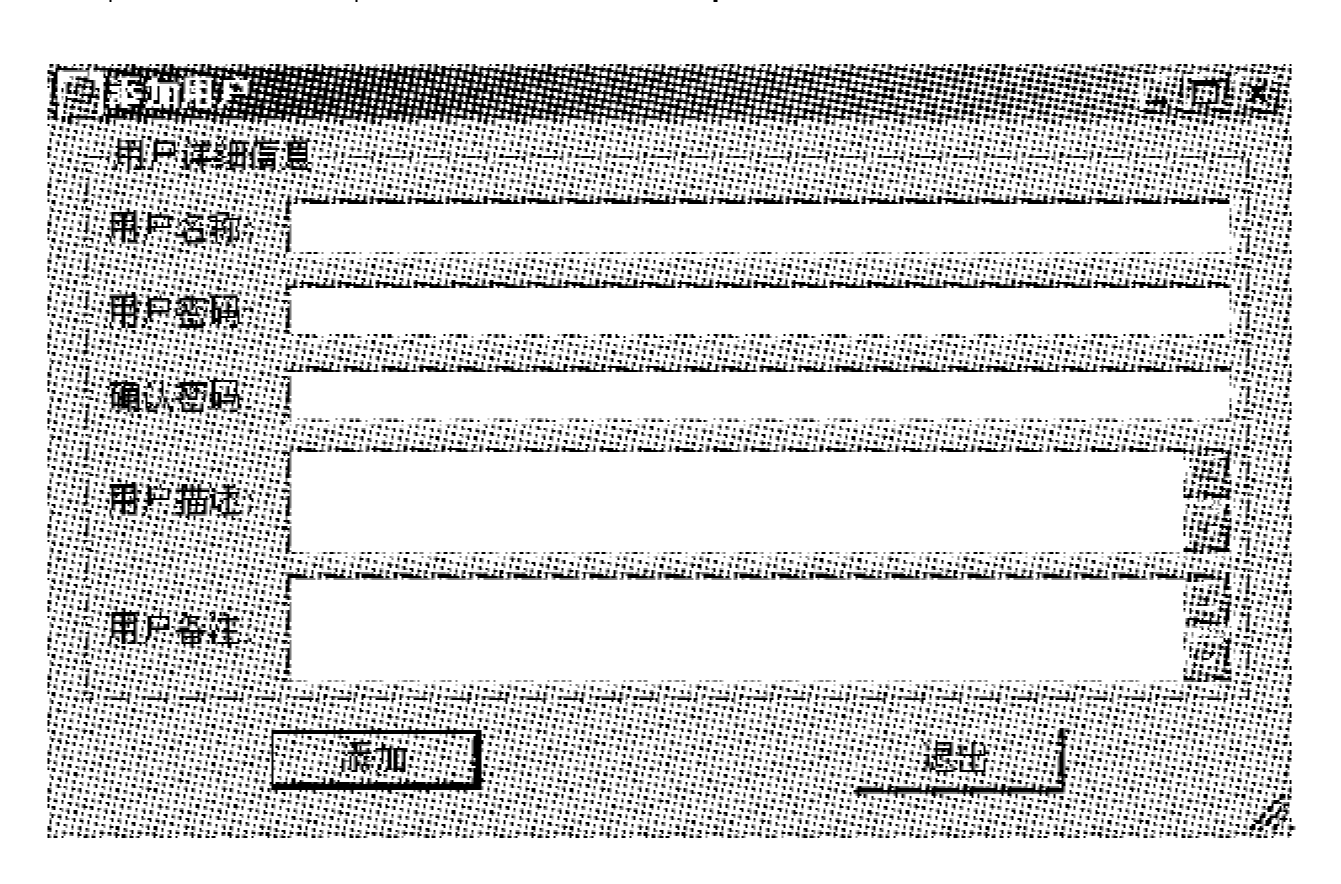



图 5-10　“添加用户”对话框

用户在此输入要添加的用户名称、用户密码、用户描述和用户备注等信息，然后单击“添加”按钮即完成了用户的添加。

用户添加完毕后，可单击“退出”按钮返回“用户管理”界面。

• 修改用户

在“用户管理”界面选中要修改的用户，单击“修改”按钮，将弹出“修改用户信息”对话框，如图 5-11 所示。

对用户名称、密码、用户描述及用户备注等信息进行修改后，单击“确定”按钮即可完成用户信息的修改，单击“退出”按钮放弃对用户信息的修改。

• 删除用户

在“用户管理”界面选中要删除的用户，单击“删除”按钮，完成对用户的删除操作。

② 用户自管理

“用户自管理”主要是对当前用户自身信息的修改。

单击“用户管理”|“用户自管理”菜单或单击快捷工具栏上的“ ”图标，系统将弹出“用户自管理”对话框，如图 5-12 所示。

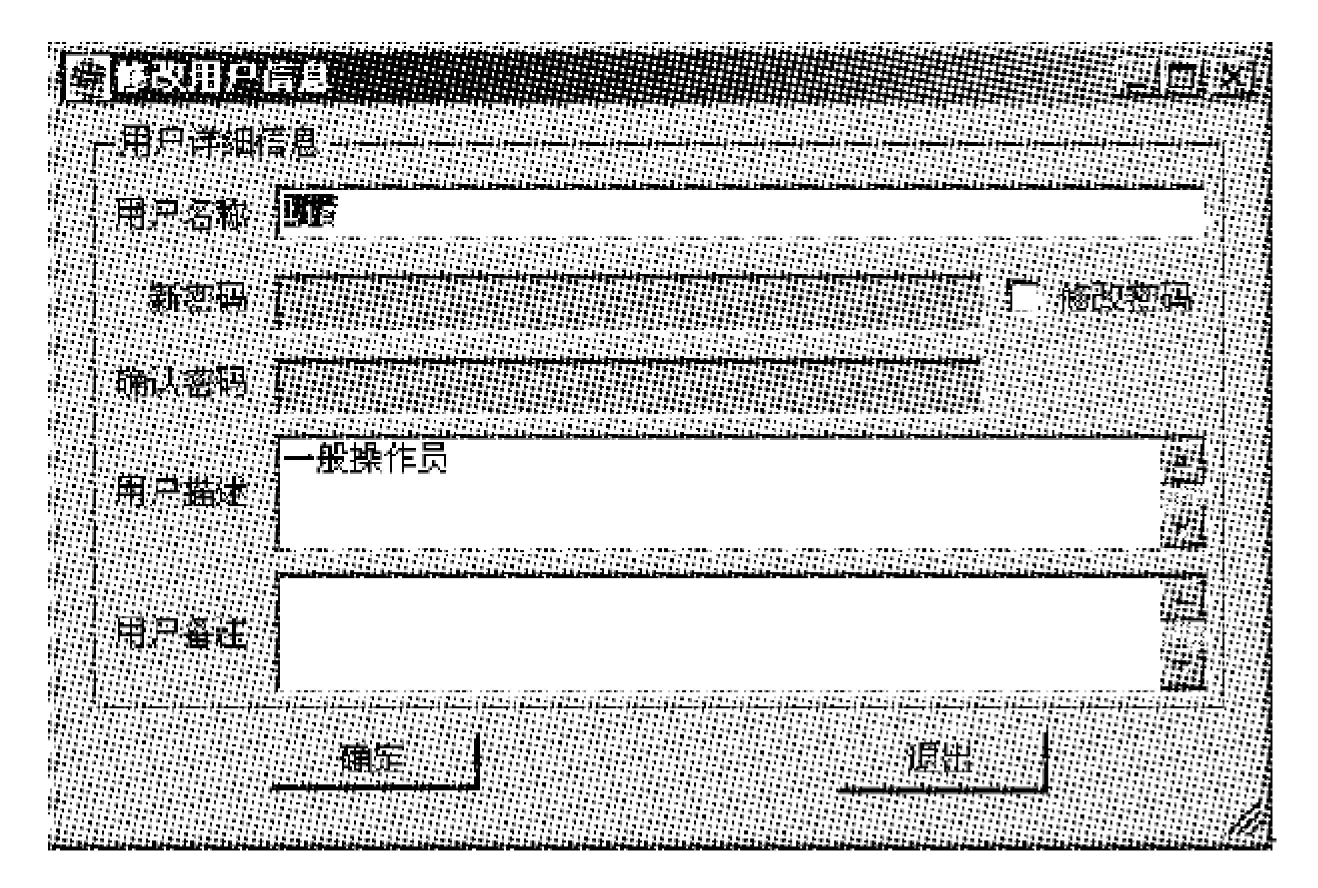



图 5-11 “修改用户信息”对话框

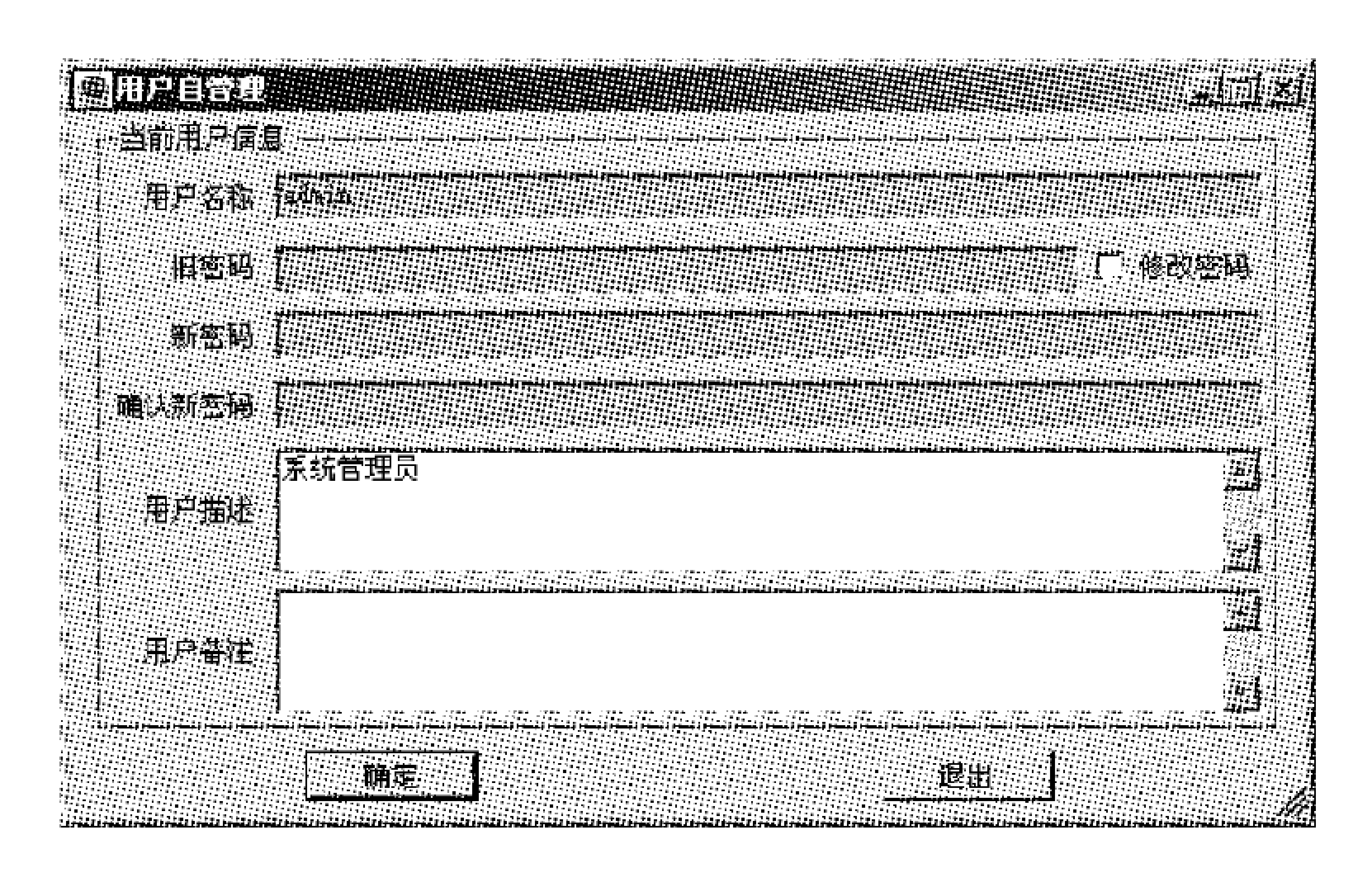



图 5-12 “用户自管理”对话框

在此对话框中对当前用户名称、密码、用户描述及用户备注等信息进行修改后，单击“确定”按钮完成当前用户信息的修改，或单击“退出”按钮放弃对当前用户信息的修改。

(2) 项目信息管理

“项目信息管理”为系统中全部项目的信息管理，功能主要包括：项目的添加、项目信息的查看、项目的修改、项目的删除等。

单击“项目管理”|“项目信息管理”菜单或单击快捷工具栏上的“”图标，系统将弹出“项目信息管理”对话框。项目信息管理模块包含项目信息的添加、修改和删除操作。

• 添加项目

单击“添加”按钮，系统将弹出“添加项目”对话框，如图 5-13 所示。

用户在此处输入项目编号、项目等级、项目名称、项目创建时间、负责人、委托单位、检测单位、整体描述和备注信息后，单击“确定”按钮即可完成项目的添加，或单击“取消”按钮放弃添加项目。

• 修改项目

在项目列表中选中要修改的项目，单击“修改”按钮，系统将弹出“编辑项目”对话框，如图 5-14 所示。

添加项目
项目编号　项目等级
项目名称
创建时间 2008-10-14 11:52:24　负责人 -----请选择项目负责人-----
委托单位　检测单位
整体描述
备注
确定　取消

图 5-13　“添加项目”对话框

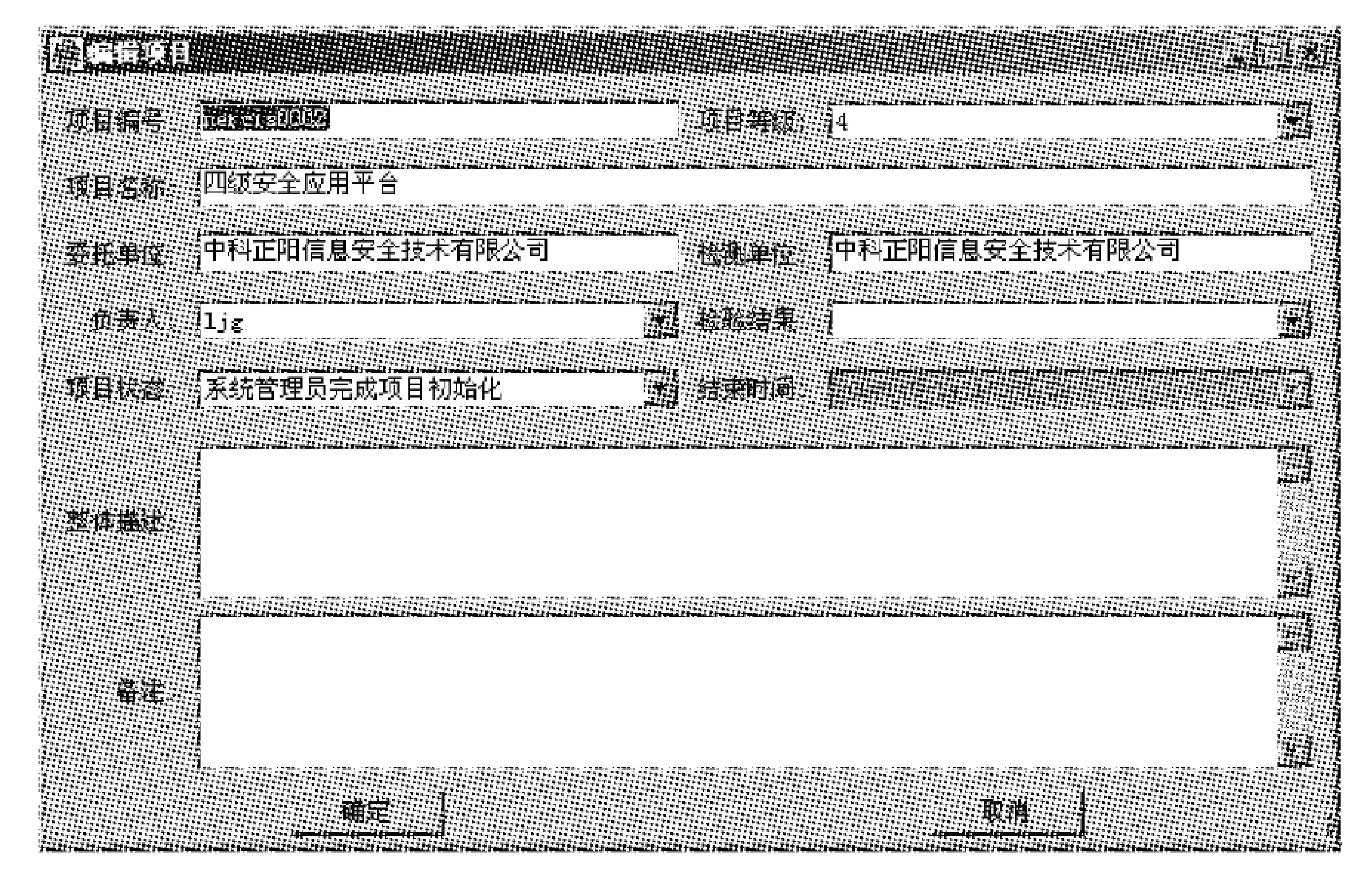



图 5-14　“编辑项目”对话框

用户在此处修改项目编号、项目等级、项目名称、委托单位、负责人、检测单位、整体描述和备注等信息后，单击“确定”按钮完成项目的修改，或单击“取消”按钮放弃项目的修改。

• 删除项目

在项目列表中选中要删除的项目，单击“删除”按钮，完成项目的删除。

### 2. 普通用户功能模块

(1) 系统登录

以普通检验人员身份登录后，可看到系统主要包括创建项目任务、项目管理、检验管理、数据分析和结果管理等功能。

根据被检验安全应用平台等级的不同，操作员可以在登录界面中选择不同等级平台

进行登录。

(2) 创建项目任务

“创建项目任务”主要包括“导入节点信息”和“添加审计事件”。

单击“文件”|“创建项目任务”菜单或单击快捷工具栏上的“ ”图标，系统将弹出“创建项目任务——导入节点信息”对话框，如图 5-15 所示。

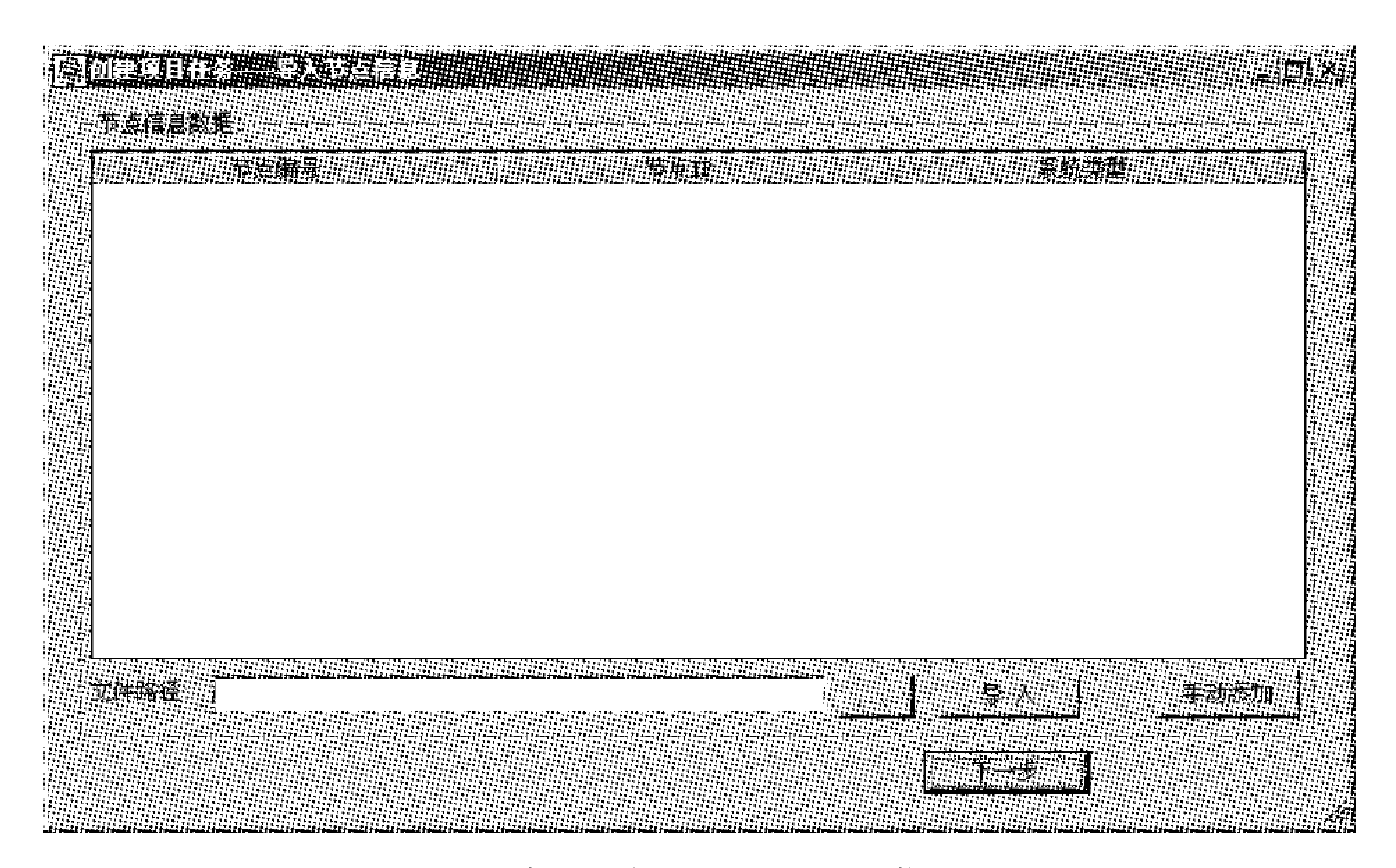



图 5-15 “创建项目任务—导入节点信息”对话框

① 导入项目节点信息

单击“...”按钮，弹出“打开”文件对话框，选择要导入的节点信息文件(XML 文件)，然后单击“打开”按钮以设定文件路径，单击“导入”按钮，完成项目中节点信息的导入。

② 手动添加

单击“手动添加”按钮，系统将弹出“添加节点信息”对话框，如图 5-16 所示。

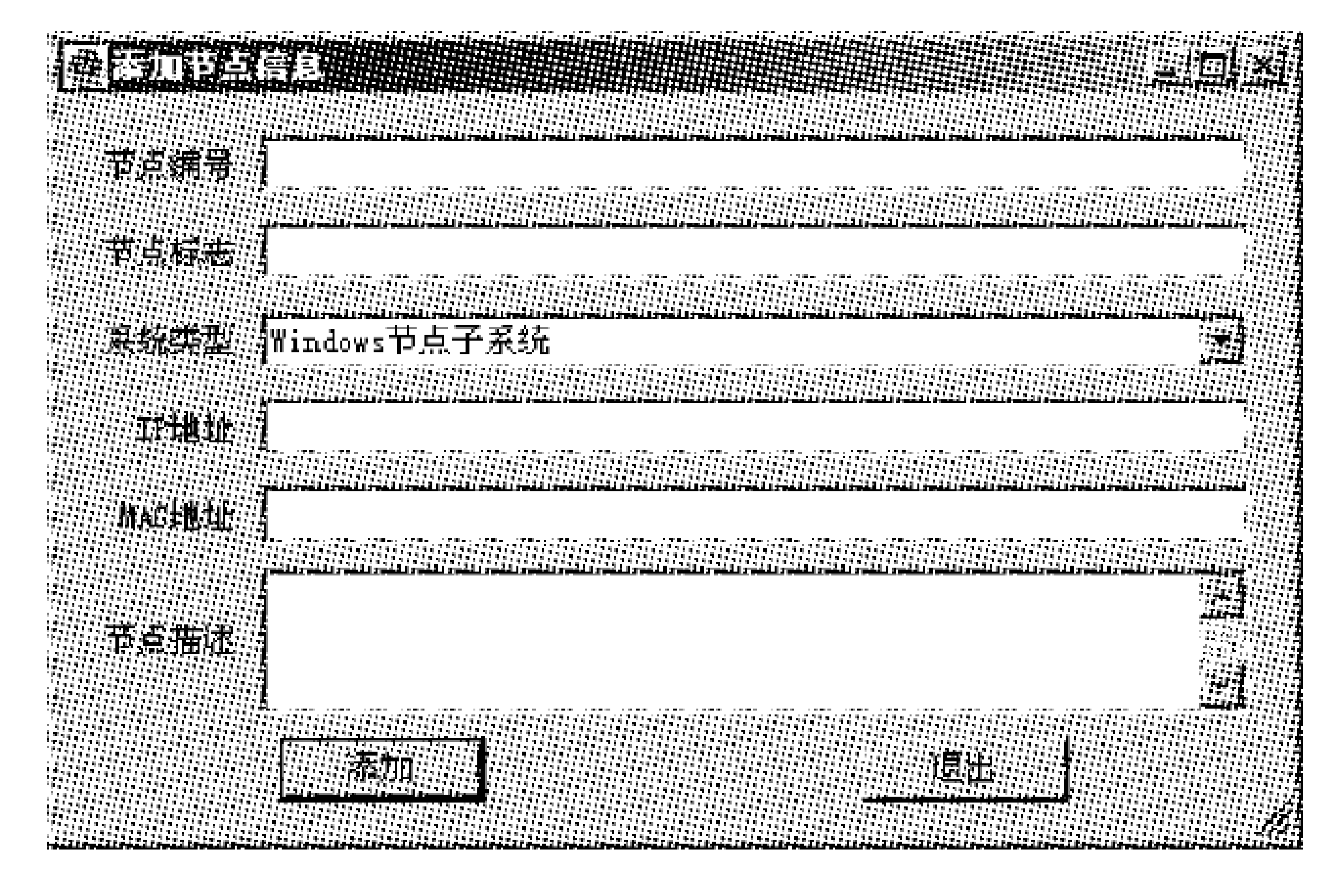



图 5-16 “添加节点信息”对话框

用户在此处输入节点编号、节点标志、系统类型、IP 地址、MAC 地址、节点描述信息后，单击“添加”按钮完成单个节点的添加，通过重复上述操作，来完成多个节点的添加。

③ 添加项目审计事件

单击“创建项目任务——导入节点信息”对话框中的“下一步”按钮，弹出“创建项目任务——添加审计事件”对话框。

根据被检验项目等级的不同，项目审计事件的类型也不相同。操作员根据提示添加系统分析所需要的审计事件对应的目标系统审计事件。下面以二级安全应用平台检验项目审计事件添加为例进行说明。

- 添加审计事件

选择左侧树中列出的系统分析所需的审计事件（以“安全计算环境子系统”|“自主访问控制功能审计事件”为例），画面如图 5-17 所示。

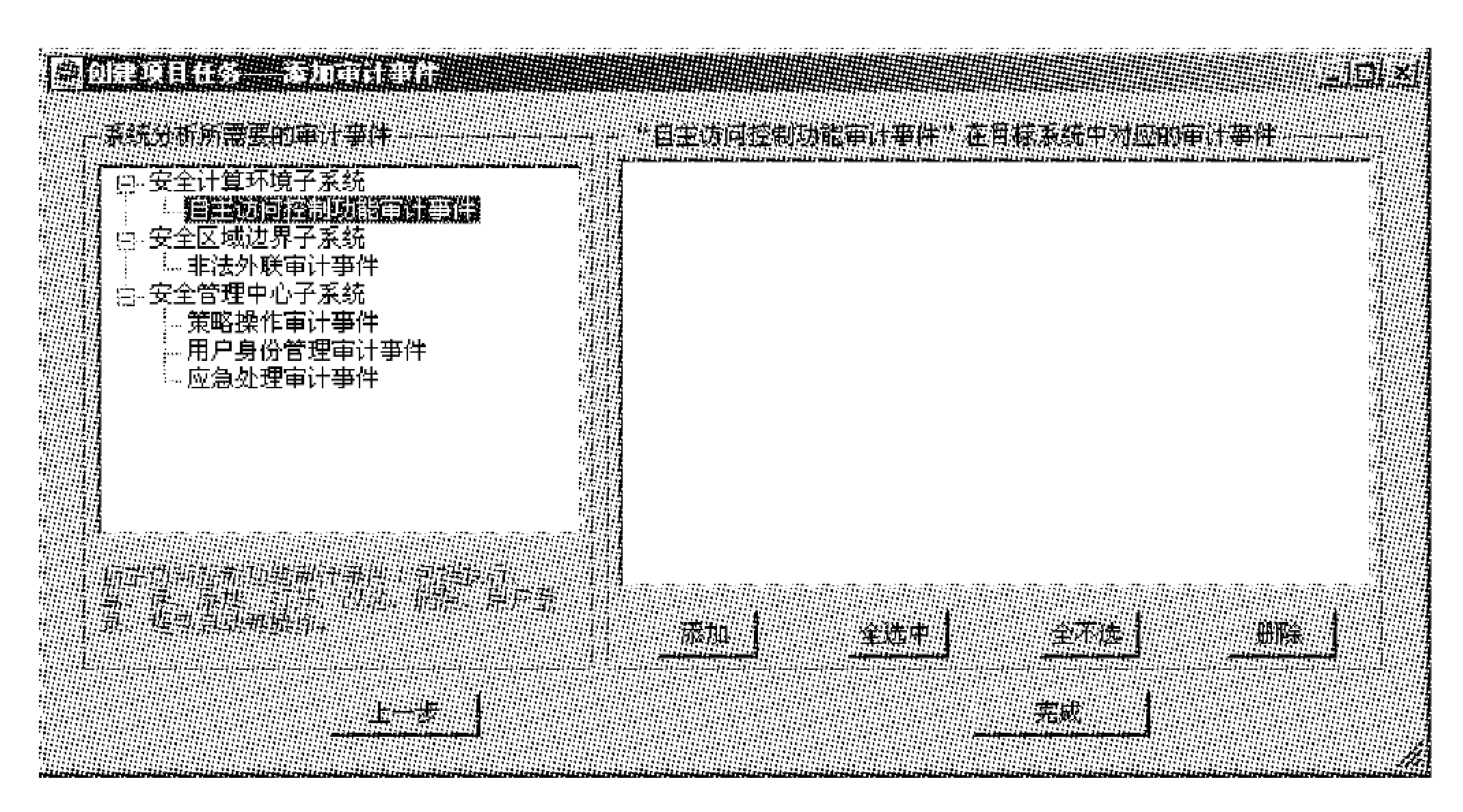



图 5-17　“自主访问控制功能审计事件”添加前的对话框

单击右侧的“添加”按钮，弹出“添加‘自主访问控制功能审计事件’的对应审计事件”对话框，如图 5-18 所示。

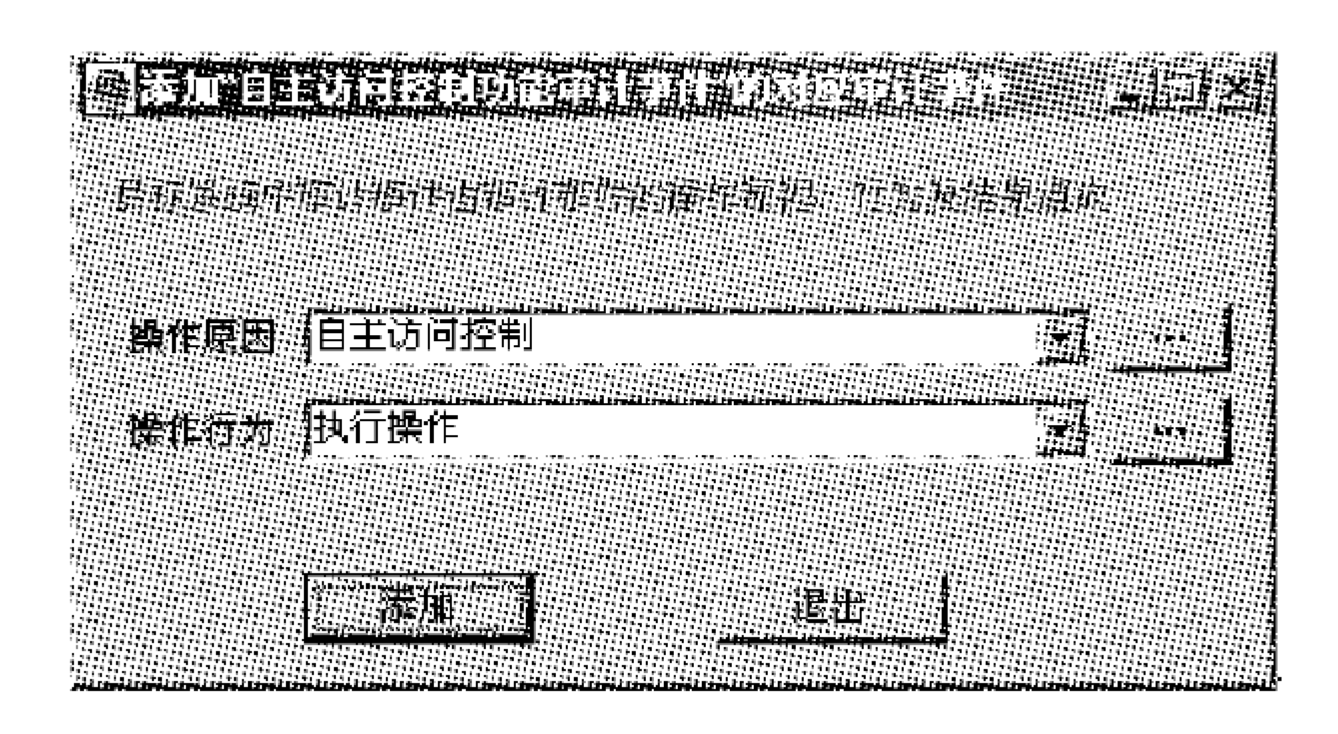



图 5-18　“添加‘自主访问控制功能审计事件’的对应审计事件”对话框

在此处选中相应的操作原因和操作行为，单击“添加”按钮，完成一个审计事件的添加，通过重复上述操作，完成多个审计事件的添加。

单击“退出”按钮退出审计事件的添加。

完成项目审计事件的添加后，如图 5-19 所示。

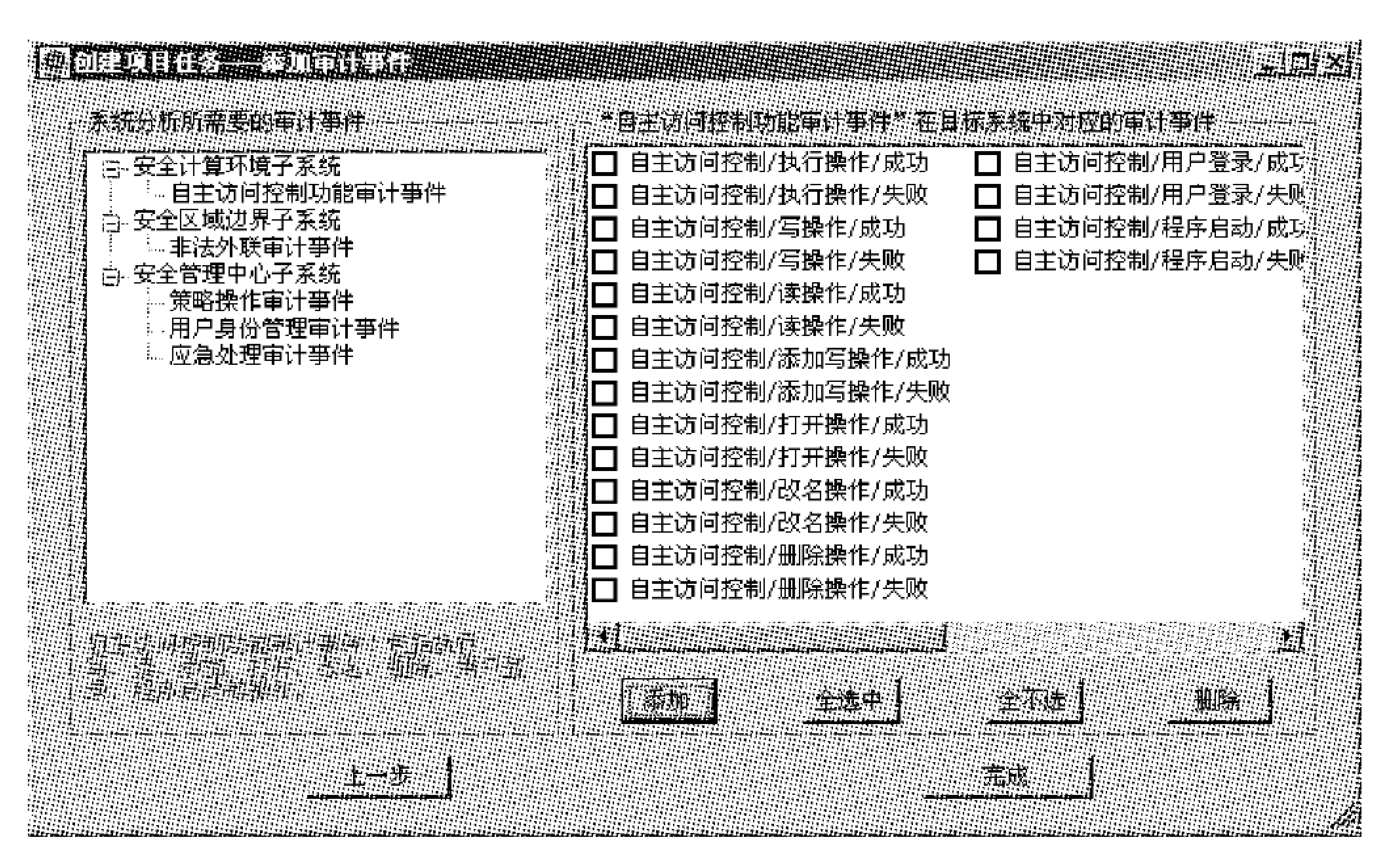



图 5-19 "自主访问控制功能审计事件"添加后的对话框

• 删除审计事件

在图 5-19 中用"√"选中右侧需要删除的审计事件(选中复选框),单击"删除"按钮,完成项目审计事件的删除。

• 添加操作原因及结果

在添加系统审计事件时,若系统提供的审计事件操作原因及结果不够全面,需要添加操作原因及结果,则单击图 5-20 中"操作原因"右侧的"..."按钮,弹出"审计事件中操作原因及结果"对话框。



图 5-20 "审计事件中操作原因及结果"管理对话框

在右侧填写操作原因名称、操作结果和原因及结果编码信息后,单击"添加"按钮,完成操作原因及结果的添加。

• 删除操作原因及结果

在图 5-20 中左侧列表中，选中要删除的项，单击“删除选中项”按钮，完成操作原因及结果的删除。

• 添加操作行为

在添加系统审计事件时，若系统提供的审计事件操作行为不够全面，需要添加操作行为，则单击图 5-18 中“操作行为”右侧的“...”按钮，弹出“审计事件中操作行为”对话框，如图 5-21 所示。

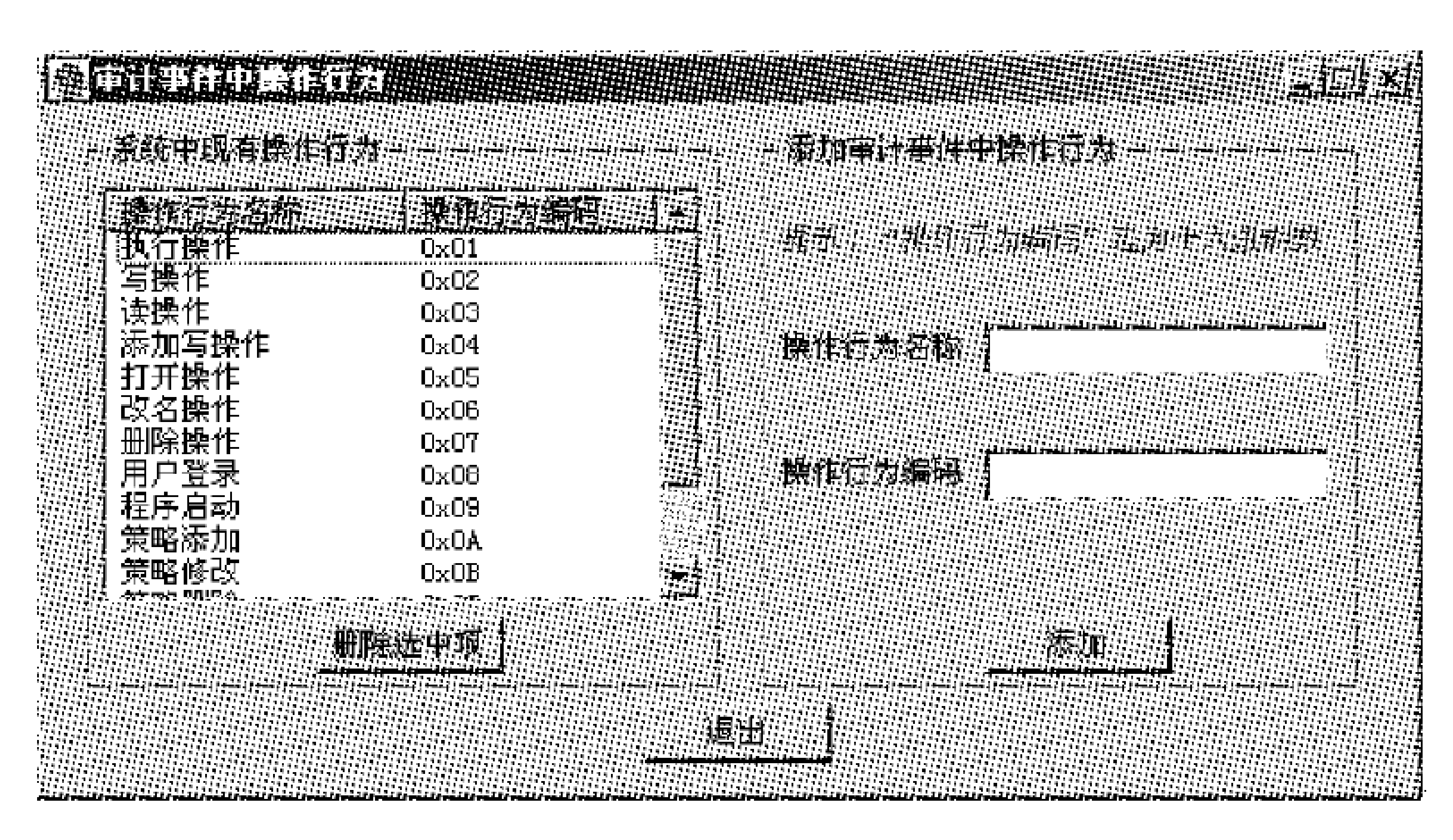



图 5-21　“审计事件中操作行为”对话框

在右侧填写操作行为名称和操作行为编码信息后，单击“添加”按钮，完成操作行为的添加。

• 删除操作行为

在图 5-21 的左侧列表中，选中要删除的项，单击“删除选中项”按钮，完成操作行为的删除。

(3) 项目管理

“项目管理”包括“项目信息管理”、“项目节点管理”和“审计事件管理”。

① 项目信息管理

“项目信息管理”为当前用户所负责的项目的信息管理，功能主要包括项目信息的查看、项目的修改、设定为待分析项目及退出等功能。

单击“项目管理”|“项目信息管理”菜单或单击快捷工具栏上的“”图标，系统将弹出“项目信息管理”对话框，如图 5-22 所示。

• 查看项目信息

单击项目列表中的某一项目，在下面的“项目其他信息”选项区查看其他相关信息。

• 修改项目

在项目列表中选中要修改的项目，单击“修改”按钮，系统将弹出“编辑项目”对话框，如图 5-23 所示。

用户在此处修改项目编号、项目等级、项目名称、委托单位、负责人、检测单位、整体描述和备注等信息后，单击“确定”按钮完成项目的修改，或单击“取消”按钮放弃项目的修改。

图 5-22 “项目信息管理”对话框

图 5-23 “编辑项目”对话框

• 设定为待分析项目

在图 5-22 项目列表中选中要进行分析的项目，单击“设定为待分析项目”按钮，完成当前检验项目的设定。

② 项目节点管理

“项目节点管理”主要包括当前项目中节点的添加、删除、信息查看及退出管理等功能。

单击“项目管理”|“项目节点管理”菜单或单击快捷工具栏上的“”图标，系统将弹出“XX 节点管理”对话框，如图 5-24 所示。

• 添加

单击“添加”按钮，系统将弹出“添加节点信息”对话框，如图 5-25 所示。

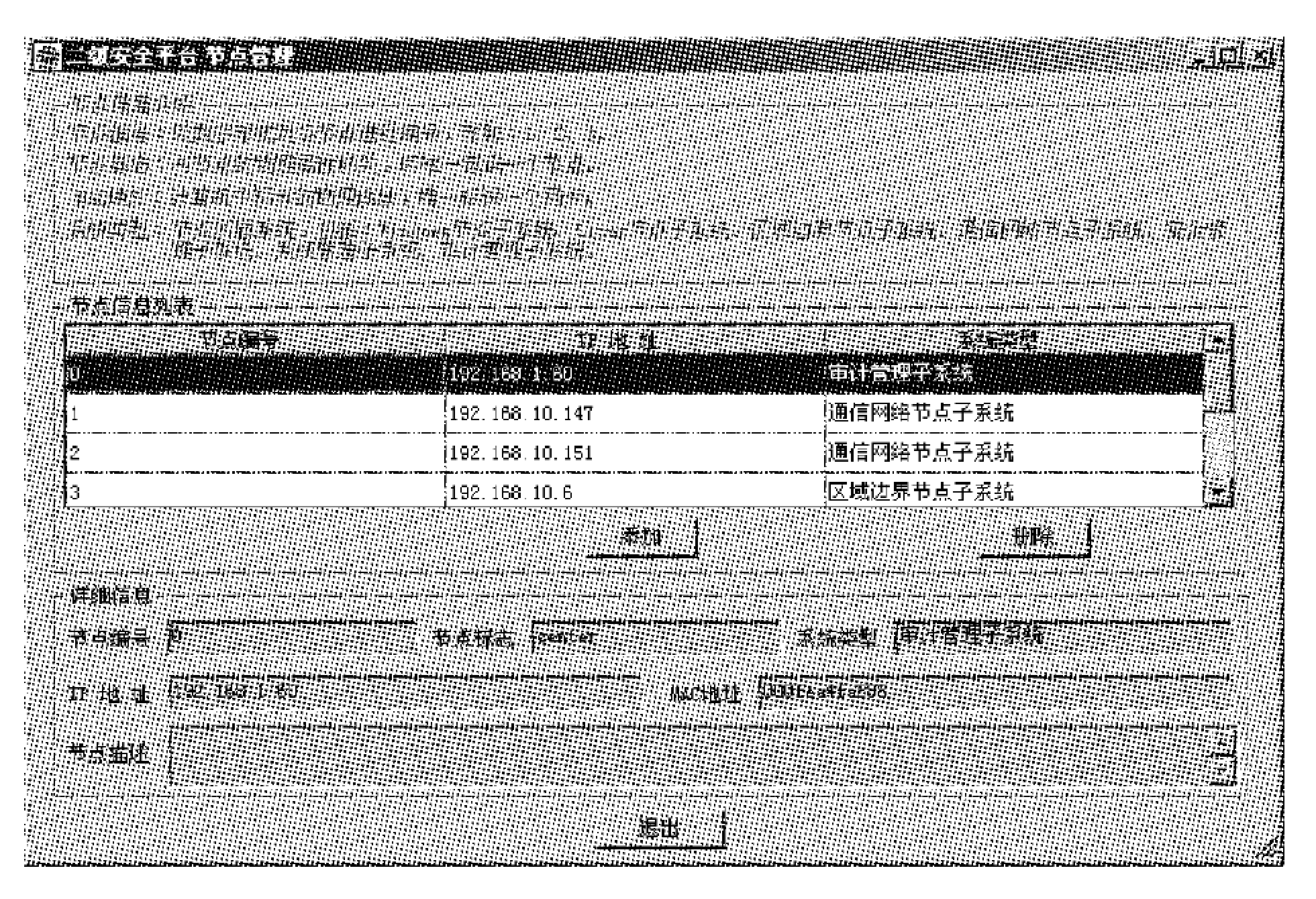



图 5-24　项目节点管理对话框

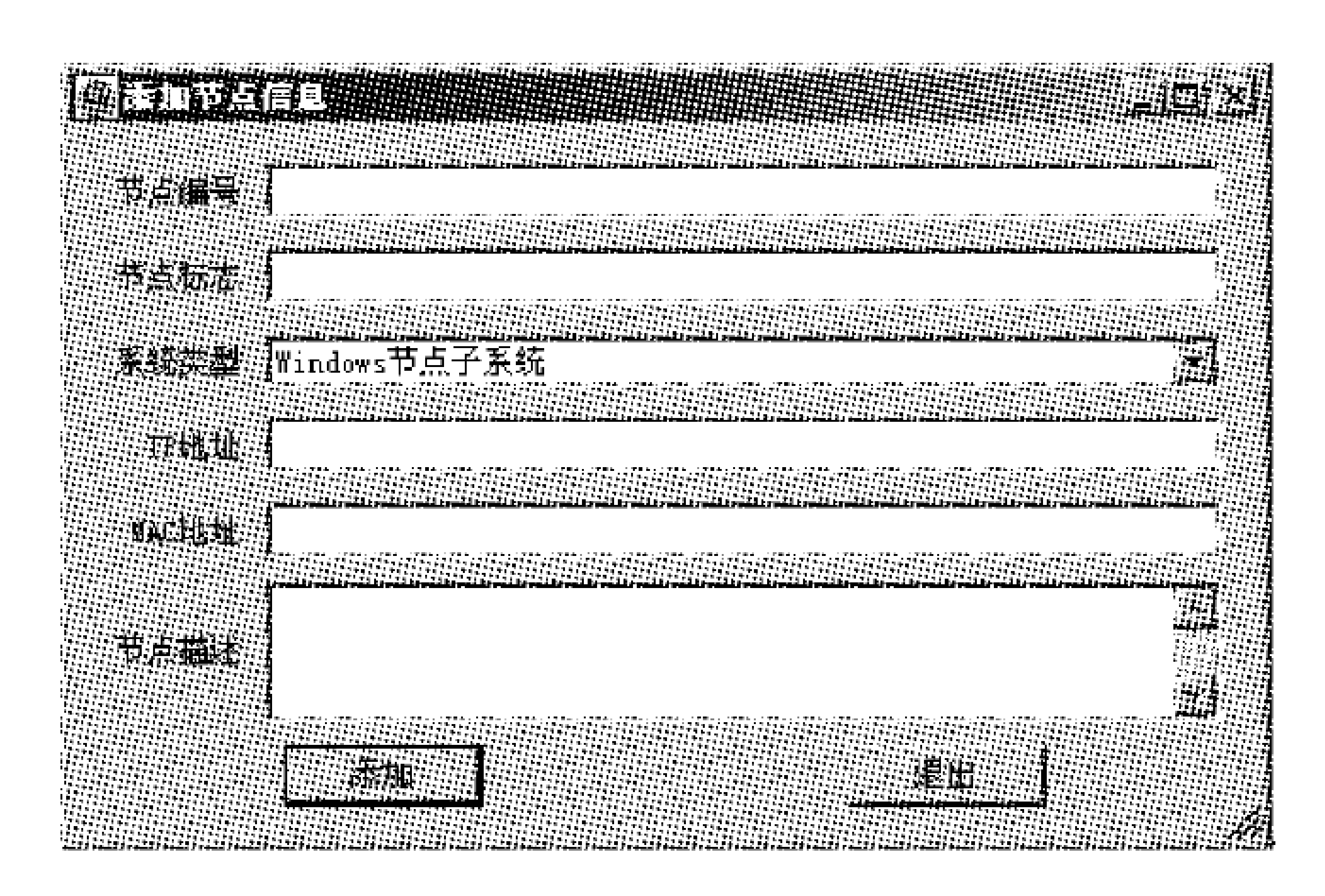



图 5-25　“添加节点信息”对话框

用户在此处输入节点编号、节点标志、系统类型、IP 地址、MAC 地址、节点描述等信息后，单击“添加”按钮完成单个节点的添加，通过重复上述操作，完成多个节点的添加。

• 删除

在图 5-24“项目节点管理”对话框内选中要删除的节点，单击“删除”按钮完成节点的删除。

③ 审计事件管理

“审计事件管理”主要包括目标系统中审计事件的添加和删除。

单击“项目管理”|“审计事件管理”菜单或单击快捷工具栏上的“ ”图标，系统将弹出“XX 审计事件管理”对话框，如图 5-26 所示。

(4) 检验管理

“检验管理”包括“导出手工检验方案”、“导入手工检验结果”、“批量导入(半)自动检验数据”、“分类导入(半)自动检验数据”及“清除(半)自动检验数据”等。

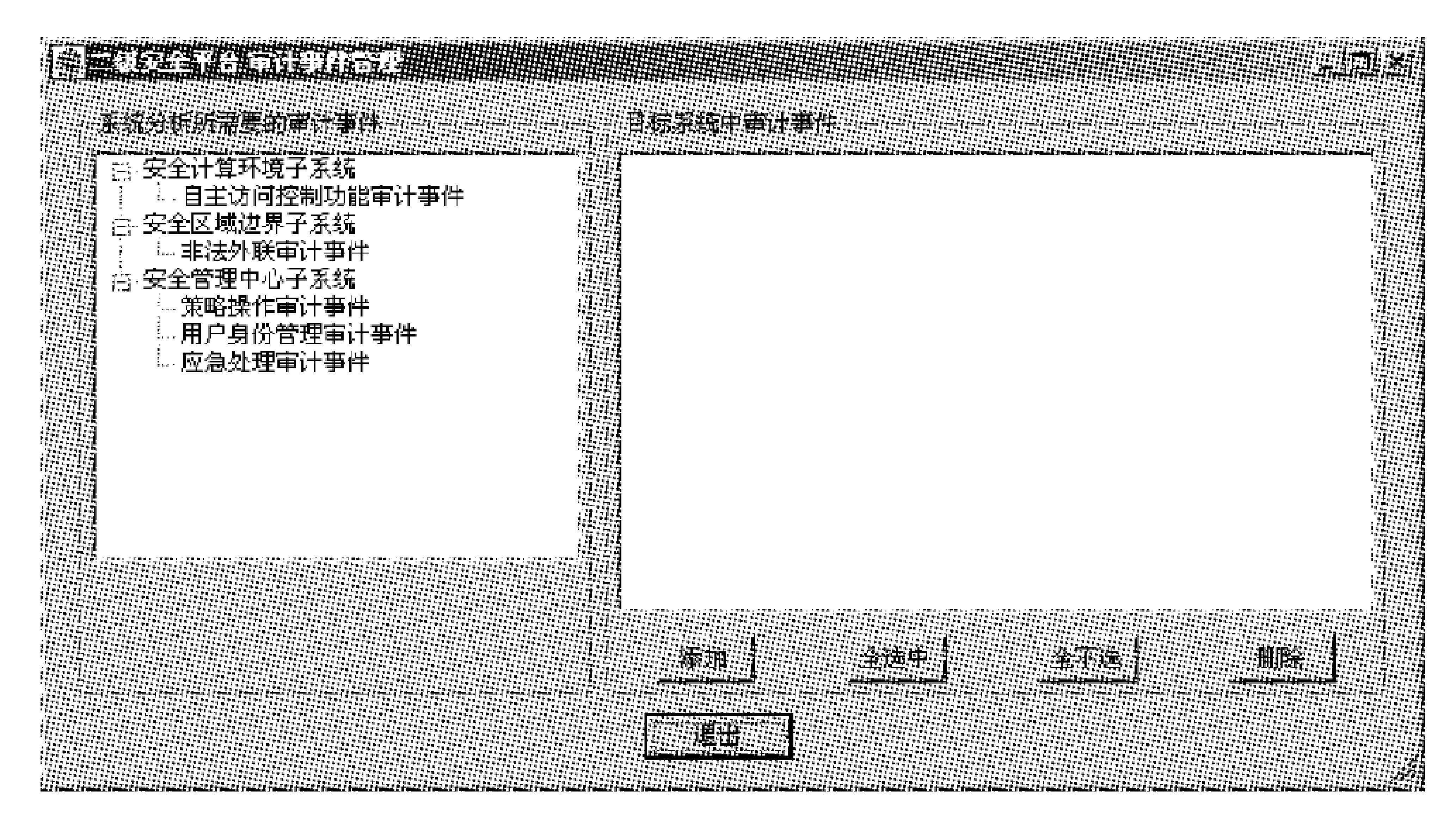



图 5-26 项目审计事件管理对话框

① 导出手工检验方案

单击“检验管理”|“导出手工检验方案”菜单，系统将弹出“导出手工检验方案”对话框，如图 5-27 所示。

单击文本框右侧的“...”按钮，弹出“另存为”文件对话框，填写要导出的手工检验方案文件(XML 文件)，单击“保存”按钮以设定图 5-27 中的文件路径，然后单击“导出手工检验方案”按钮，完成手工检验方案的导出。

单击“退出”按钮，关闭“导出手工检验方案”对话框。

② 导入手工检验结果

单击“检验管理”|“导入手工检验结果”菜单，系统将弹出“导入手工检验结果”对话框，如图 5-28 所示。

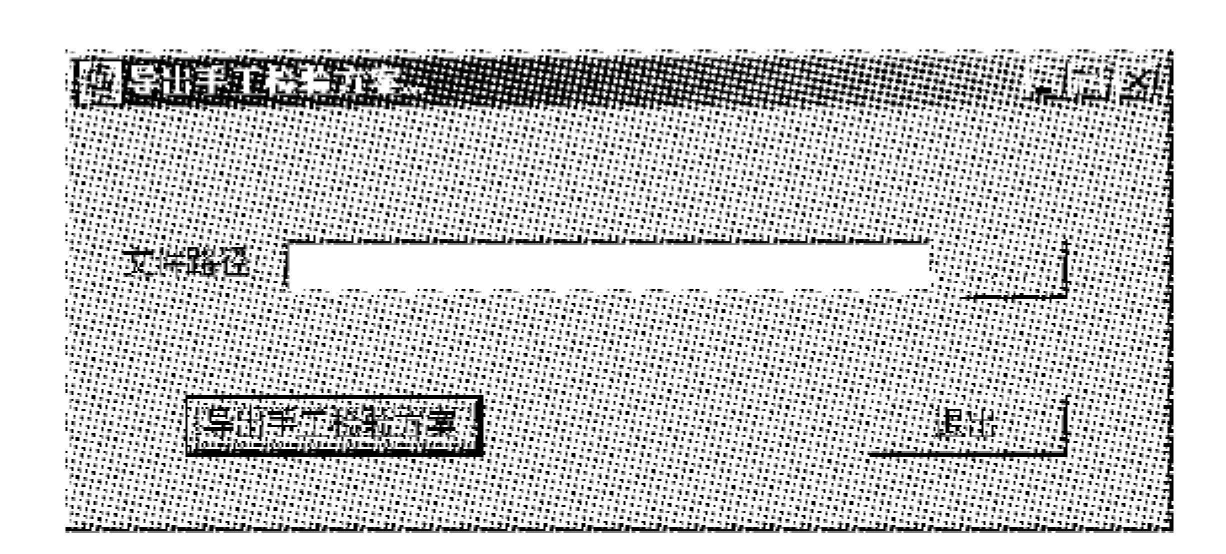


图 5-27 “导出手工检验方案”对话框

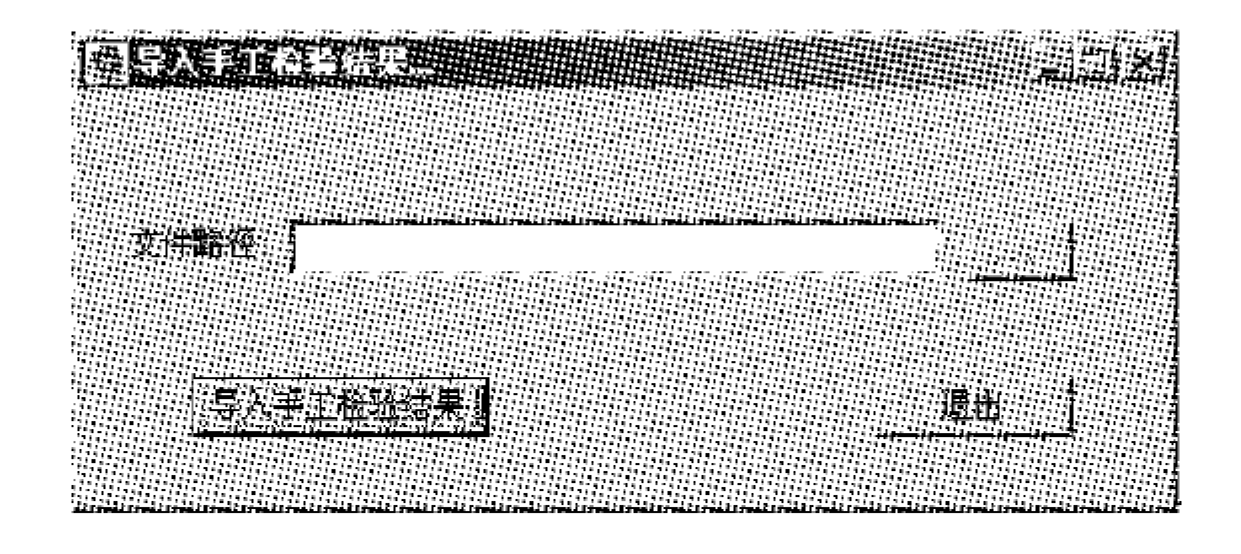


图 5-28 “导入手工检验结果”对话框

单击文本框右侧的“...”按钮，弹出“打开”文件对话框，选中需要导入的手工检验结果文件(XML 文件)，单击“打开”按钮以设定图 5-28 中的文件路径，然后单击“导入手工检验结果”按钮，完成手工检验结果的导入。

单击“退出”按钮，关闭“导入手工检验结果”对话框。

③ 批量导入(半)自动检验数据

单击“检验管理”|“导入(半)自动检验数据”菜单，系统将弹出“打开”对话框，如图 5-29 所示。

打开

查找范围(I): XML

temp
AuditInfo.XML
AuditPlcy.XML
DacFile.XML
DacFileZone.XML
NodeInfo.XML
ObjFile.XML
PrivFile.XML
SubFile.XML
transdata1.xml
transdata2.xml
transdata3.xml
transdata5.xml

文件名(N):　　打开(O)

文件类型(T): XML文件(*.xml)　　取消

图 5-29　“打开”对话框

选中需要导入的(半)自动检验数据文件(XML 文件),单击“打开”按钮批量导入(半)自动检验数据。

④ 分类导入(半)自动检验数据

分类导入(半)自动检验数据包括 Windows 计算环境数据的获取、Linux 计算环境数据的获取、单个计算节点数据的获取、安全区域边界子系统数据的获取、安全通信网络子系统数据的获取、安全管理子系统数据的获取(三/四级)、系统管理子系统数据的获取、审计管理子系统数据的获取等。每个子系统的数据获取操作流程基本相同,下面以 Windows 计算环境数据的获取为例进行操作演示。

单击主界面左侧树中“安全计算环境子系统”,选择右侧“Windows 计算环境数据获取”属性页,界面如图 5-30 所示。

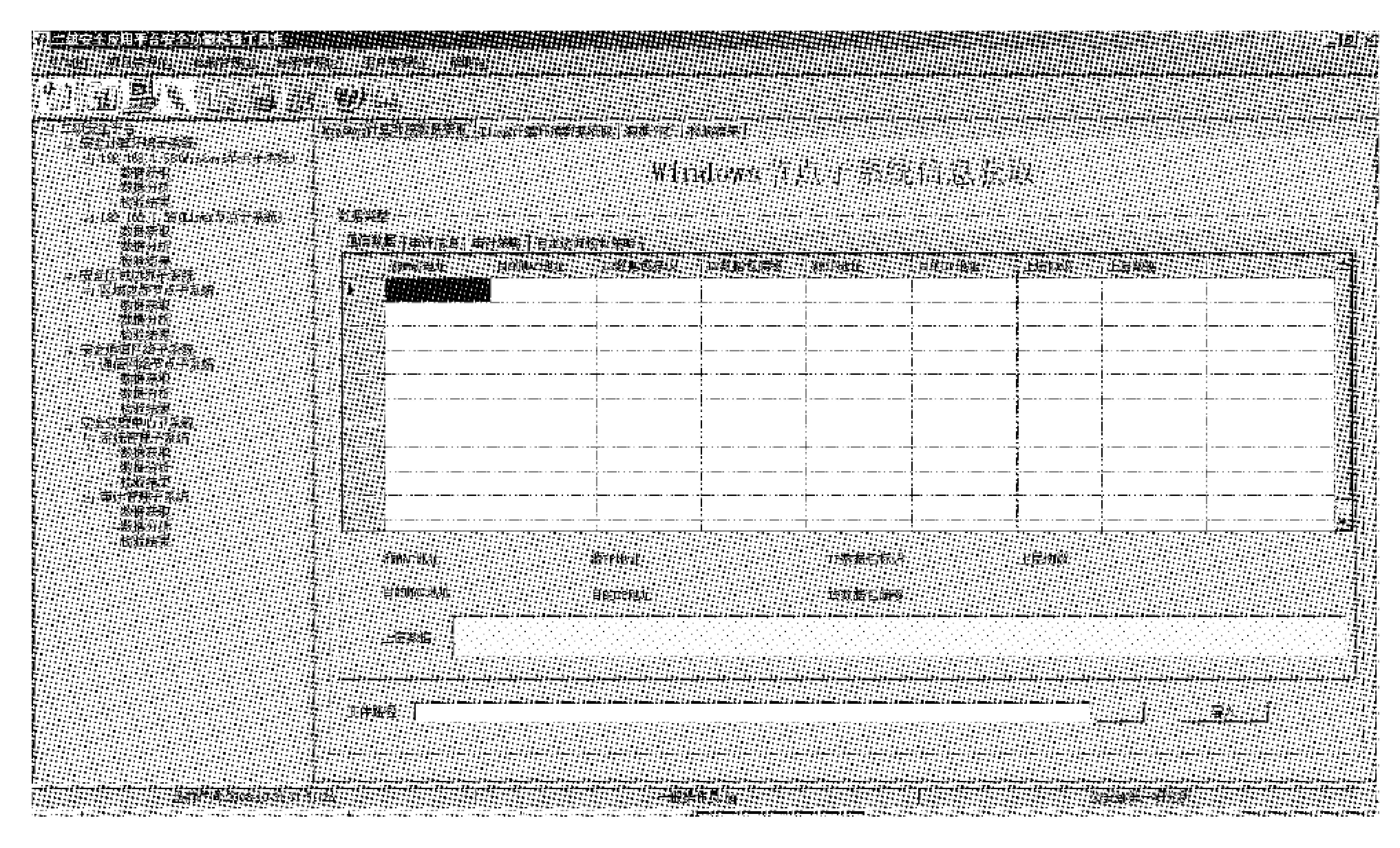


图 5-30　Windows 计算环境数据获取界面

选中右侧界面中“数据类型”内的“通信数据”属性页，单击“Windows 计算环境数据获取”属性页下方的“...”按钮，弹出“打开”文件对话框，选中需要导入的检验数据（XML 文件），单击“打开”按钮以设定文件路径，然后单击“导入”按钮，完成 Windows 计算环境中通信数据的获取。

Windows 计算环境中其他数据的获取类似。

⑤ 清除（半）自动检验数据

单击“检验管理”|“清除（半）自动检验数据”菜单，系统将弹出“清除检验数据...”对话框，选中需要清除的数据的复选框，然后单击“清除数据”按钮完成相应的操作，如图 5-31 所示。

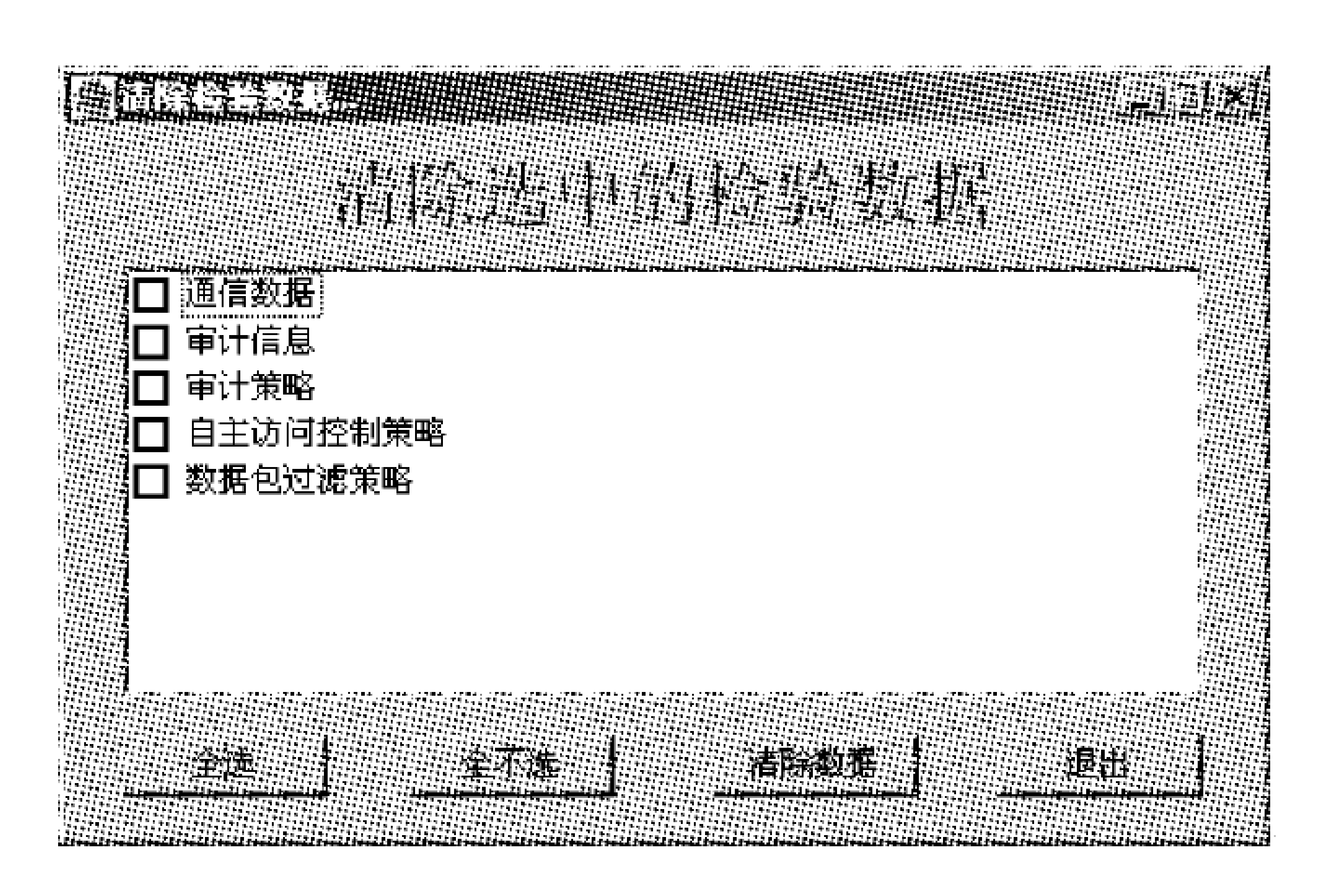



图 5-31 “清除检验数据”对话框

(5) 数据分析

“数据分析”包括 Windows 计算环境数据分析、Linux 计算环境数据分析、单个计算节点数据分析、安全区域边界子系统数据分析、安全通信网络子系统数据分析、安全管理子系统数据分析（三/四级）、系统管理子系统数据分析、审计管理子系统数据分析等。

每个子系统的数据分析操作流程基本相同，下面主要以安全计算环境数据分析操作流程为例进行演示。

① 安全计算环境数据分析

单击主界面左侧树中“安全计算环境子系统”，选择右侧“数据分析”属性页，界面如图 5-32 所示。

用“√”选中右侧界面中需要分析的节点（复选框），单击“开始分析”按钮，将依次完成对各个检验要素的分析。

② 单个计算节点数据分析

单击主界面左侧树中“安全计算环境子系统”中单个节点下的“数据分析”选项，界面如图 5-33 所示。

可以通过选中右侧区域中各个属性页中的检验要素来确定要检验的内容，然后单击“开始分析”按钮进行数据分析。

图 5-32　安全计算环境数据分析界面

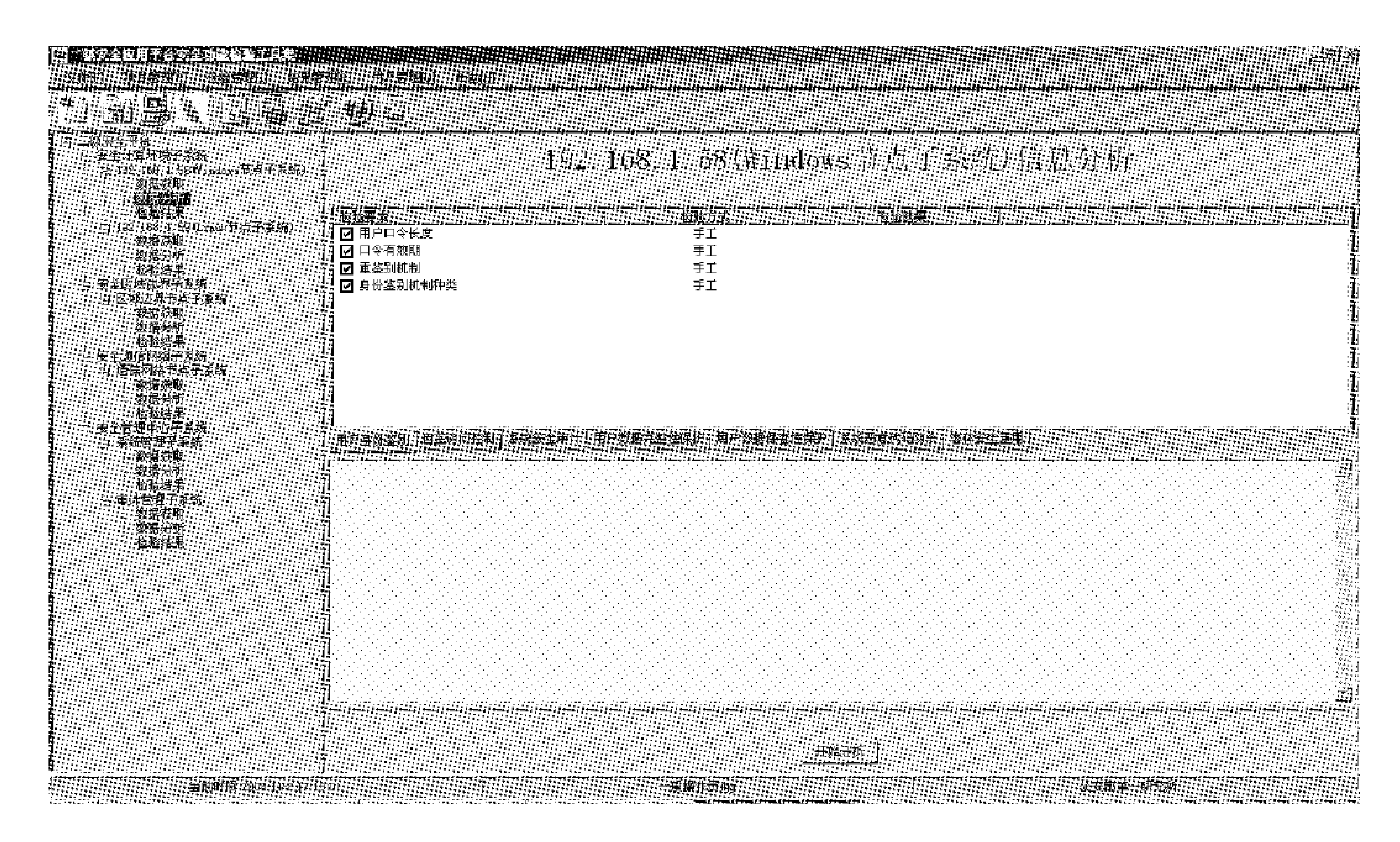


图 5-33　单个计算节点数据分析界面

(6) 结果管理

“结果管理”既可以查看总体的检验结果，也可以单独查看某一子系统或某一节点的检验结果，并能生成检验报告。

① 总体结果查看

单击“结果管理”|“查看结果”菜单，或单击快捷工具栏上的“ ”图标，界面如图 5-34 所示。

② 各部分结果查看

在主界面左侧树中单击各个子系统(或节点)，然后单击主界面右侧中的“检验结果”

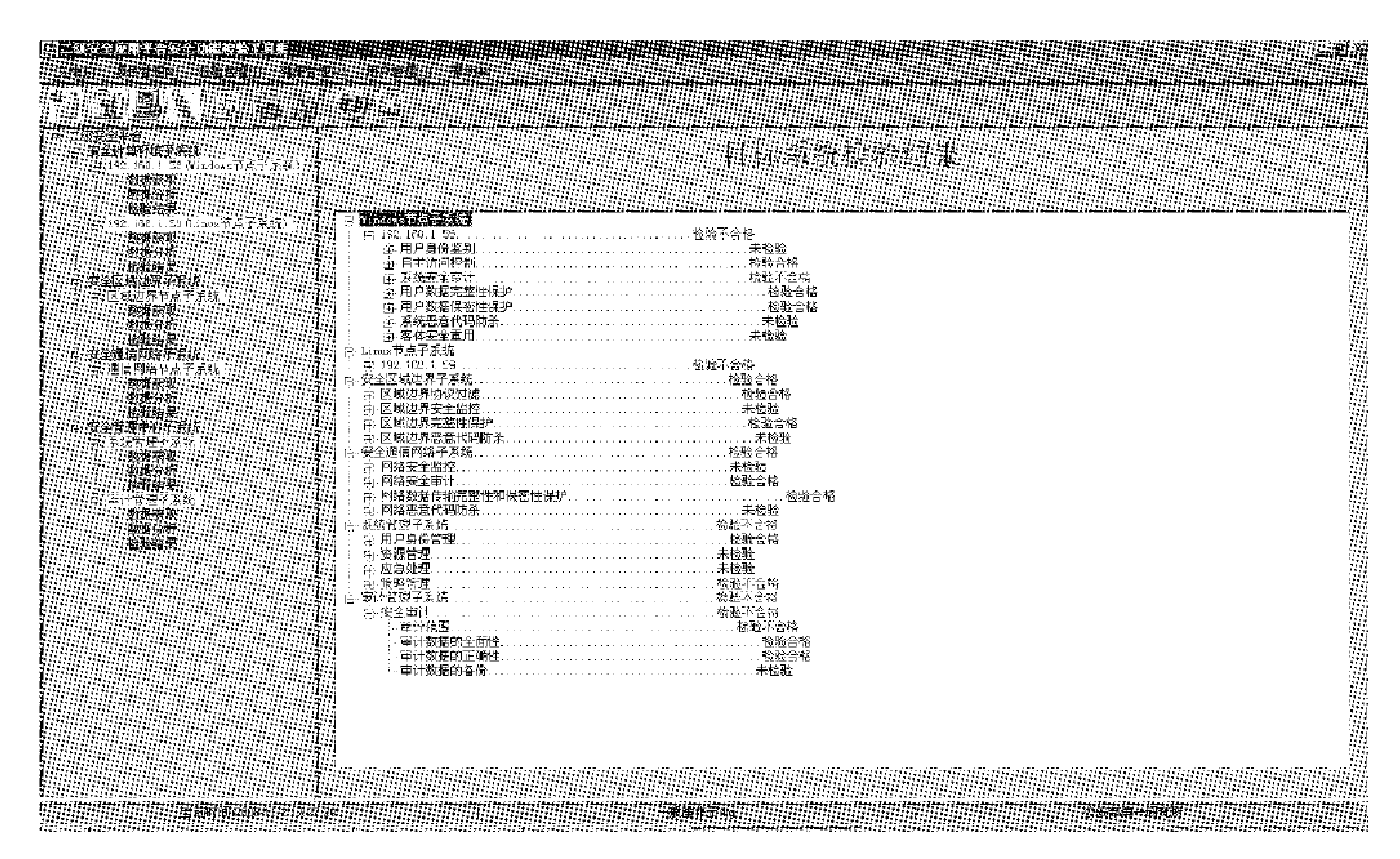


图 5-34 总体结果查看界面

属性页，将显示对应子系统（或节点）的检验结果，如图 5-35 和图 5-36 所示。

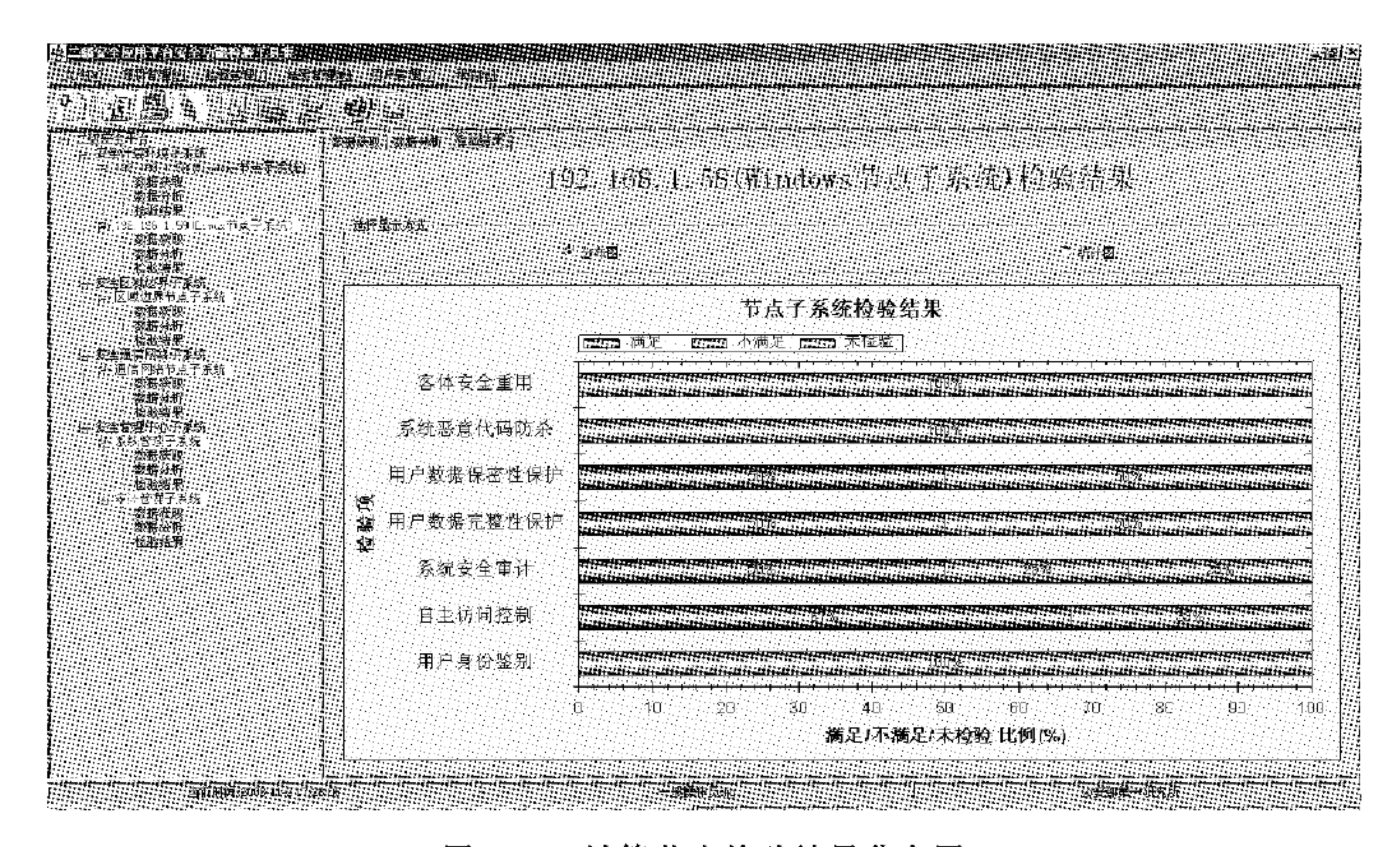



图 5-35 计算节点检验结果分布图

③ 生成报告

单击“结果管理”|“生成报告”菜单，或单击快捷工具栏上的“”图标，弹出“选择 Word 版本”对话框，如图 5-37 所示。

通过单击“是”或“否”按钮选择 Word 的版本，将弹出“报告生成”对话框，在弹出的对话框中可以选择“向导模式”或者“快速生成”模式生成相应的检验报告。

图 5-36 计算节点检验结果统计图

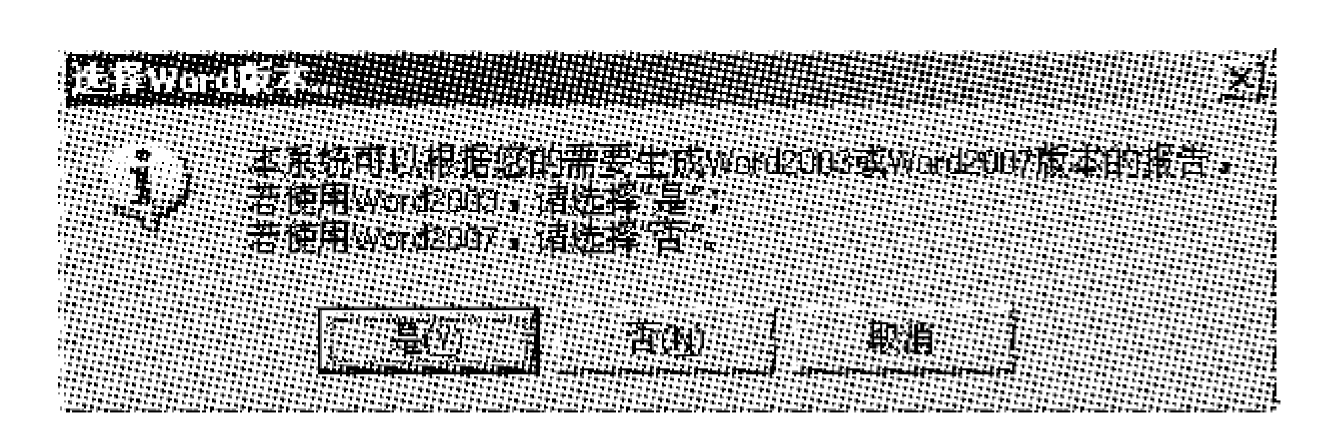



图 5-37 “选择 Word 版本”对话框

## 5.4.3 手工检查工具

手工检查工具的功能主要有：导入数据、编辑检验记录、评定检验结果和查看检验结果。

在欢迎使用对话框中单击“下一步”按钮后会看到图 5-38 所示的界面，在此选择安全平台所属的等级，否则不能进行下面的操作。

### 1. 导入数据

单击“浏览”按钮，选择要导入的 XML 文件，如果为空或者文件格式有误则会给出提示“重新导入”，如图 5-39 所示。

单击“下一步”按钮后将给出确认提示，如果确认路径正确，则单击“导入”按钮，如图 5-40 所示。

### 2. 编辑检验记录

单击“导入”按钮，出现如图 5-41 的界面。在每个检验要素的详细信息中，包含了该要素的所属子系统、所属检验项、检验要素的编号和名称、检验方法和检验记录等信息。其中“检验方法”指导用户如何去进行检验，用户可以在“检验记录”中记录检验过程中的详细信息。如果在检验过程中需要添加一些文件附件作为证据，可以单击“添加附件路径”按钮，添加相关附件。该路径将保存在 XML 文件中，以供用户作为搜寻证据的参考。

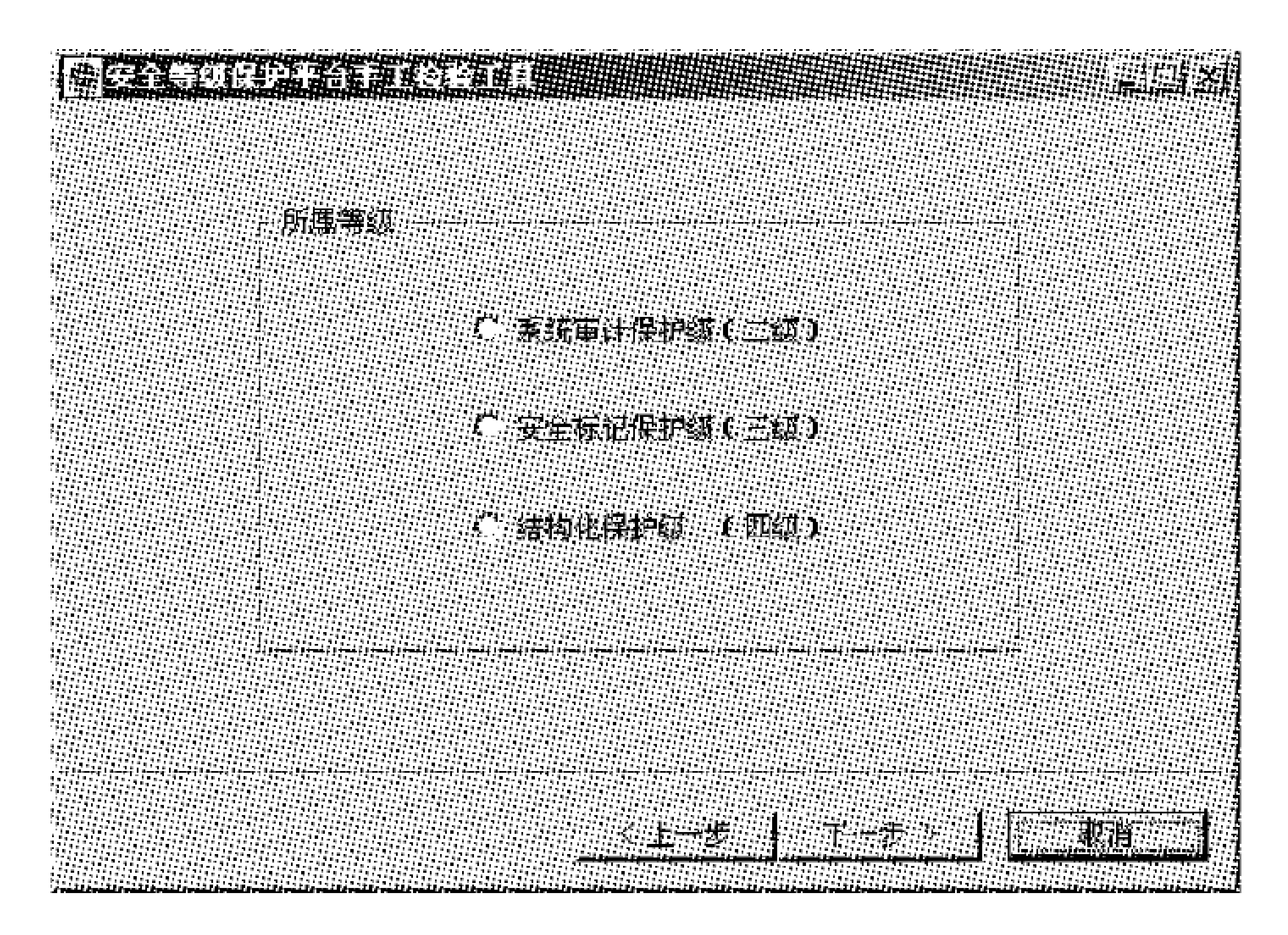



图 5-38　选择安全平台所属的等级

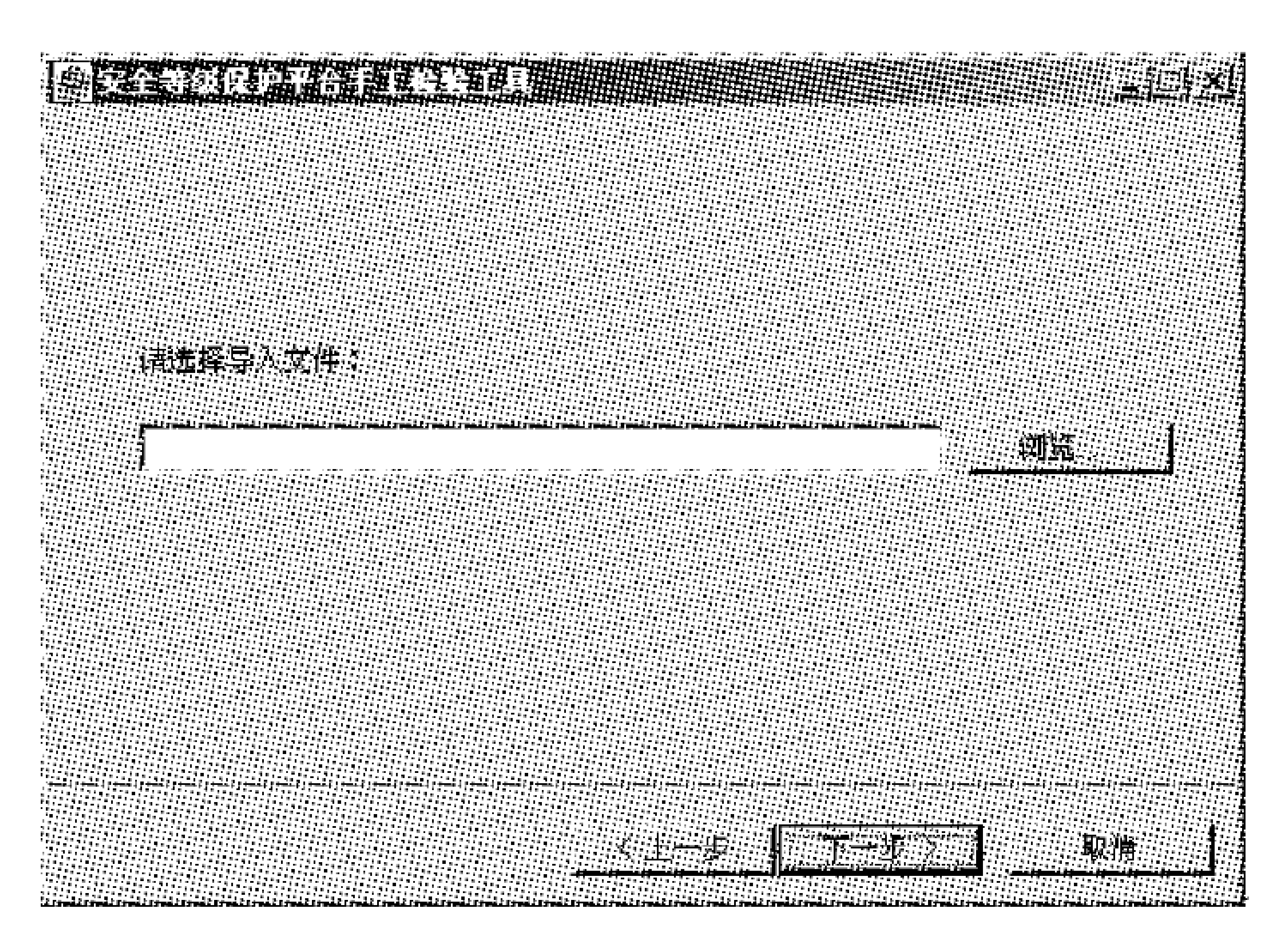



图 5-39　从 XML 文件导入数据

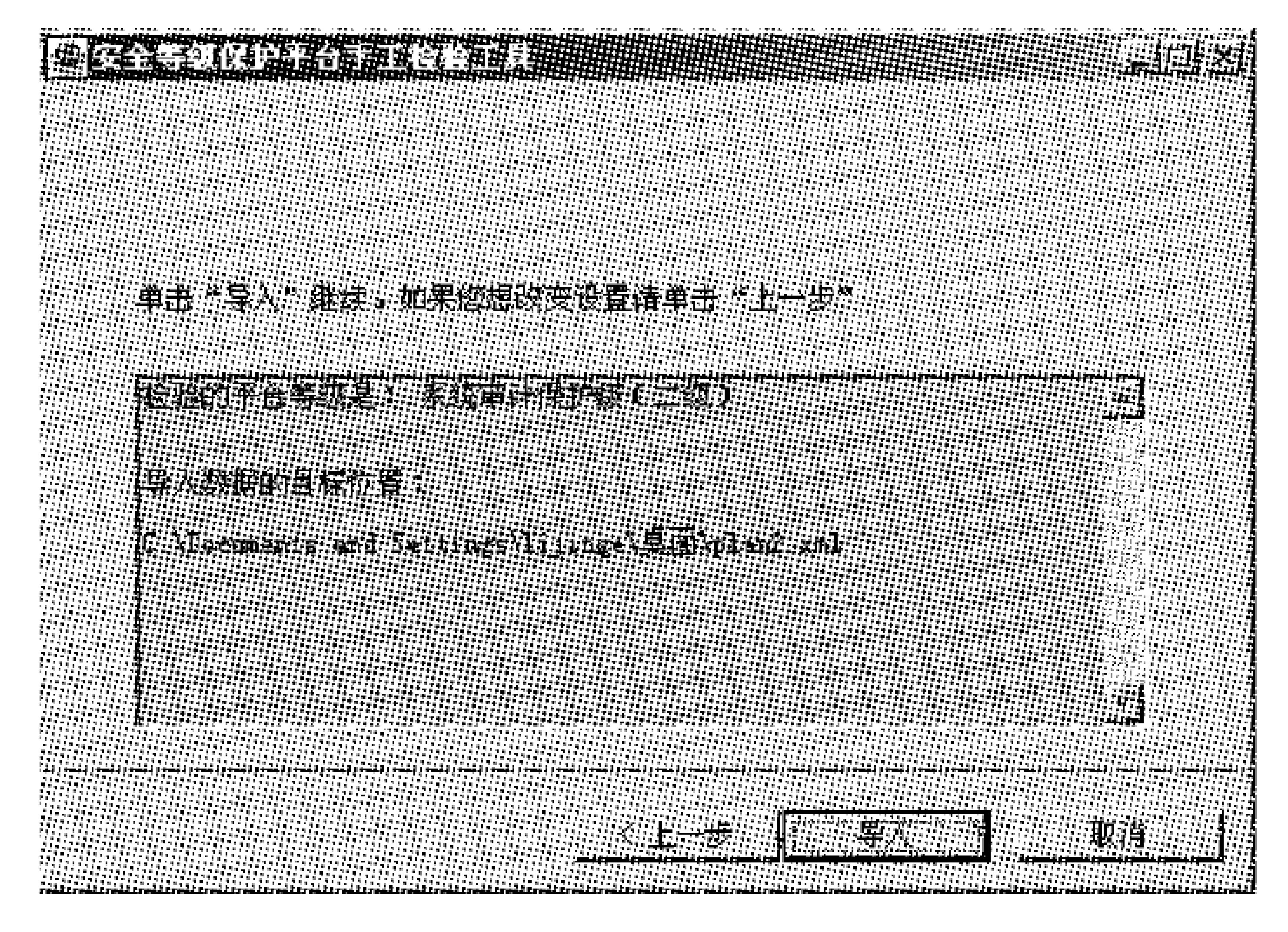



图 5-40　确认导入

图 5-41　手工检验过程

### 3. 评定检验结果

如图 5-41 所示，用户在检验每一项要素之后，根据得到的相关信息可在右下角选择该要素检验的结果(合格/不合格)。

当进行完最后一个要素的检验之后，单击“下一步”按钮将出现是否查看检验结果的提示框。

### 4. 查看检验结果

进入检验结果查看功能之后，将看到如图 5-42 所示的界面，该界面左边是一个树，包含了本次手工检验的所有子系统、检验项及其相关信息。

在树中单击“包含检验项”，会出现该子系统所包含的检验项，单击某个检验项的节点，在右边将出现该项所包含的检验要素检验结果的相关信息，其中有检验结果和检验记录，如图 5-42 所示。

## 5.4.4　设计要求检验策略库管理

“设计要求检验策略库管理系统”是为了辅助等级保护的检验工具集开发而设计的，通过“设计要求检验策略库管理系统”可以为等级保护检验工具集的开发提供需要检验的检验类、检验项、检验要素和检验方法等。

设计要求检验策略库同样分为管理员功能模块和普通用户功能模块。

管理员功能模块包含用户管理和用户自管理两个功能子模块。其中用户管理包含新

建用户、修改用户信息和删除用户信息。用户自管理主要是对管理员自身的信息进行编辑,包含口令和基本信息的修改。具体的操作流程可以参考数据分析端"系统管理员功能"章节的相关演示。

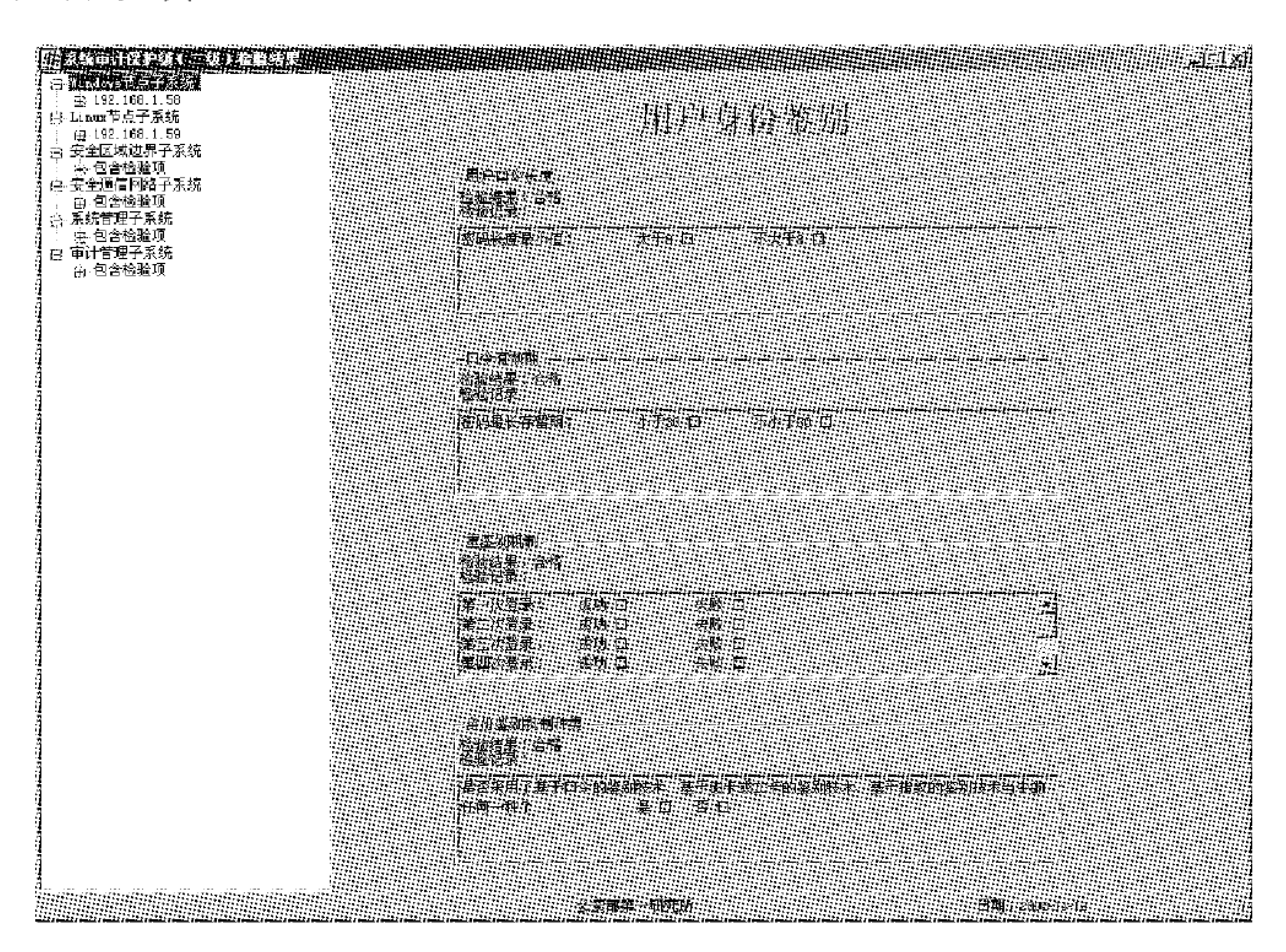



图 5-42 结果查看

普通用户功能模块主要是对检验类、检验项、检验要素以及相对应的检验方法进行管理维护。维护操作的方式主要有新建、查看、修改和删除相应的信息。下面以检验类为例进行相关的操作演示。

检验类管理主要是对要检验的类进行新建、查看、修改和删除操作的管理。

### 1. 新建检验类

在设计要求检验策略库管理主界面中的左面树中,选中检验类的上级节点右击,在弹出的快捷菜单中选择"新建检验类"命令或者在右面部分右击,在弹出的快捷菜单中选择"新建检验类"命令,还可以在上面的菜单"检验类管理"中选择"新建检验类"选项,都会看到图 5-43 所示的"新建检验类"对话框。

输入新的检验类信息后单击"确定",则新建一个检验类,否则单击"取消"按钮取消新建操作。

### 2. 查看检验类

选中左面树的某一个检验类节点右击,在弹出的快捷菜单中选择"查看检验类"命令,会看到图 5-44 所示的"查看检验类详细信息"对话框。

或者在系统主界面中,选中右面列表中某一个检验类,单击该检验类的记录,在列表下方可显示该检验类的详细信息。

在查看页面中单击“修改”按钮，会进入修改检验类信息页面(下面会详细介绍)。单击“取消”按钮返回。

图 5-43　“新建检验类”对话框

图 5-44　“查看检验类详细信息”对话框

### 3. 修改检验类

选中左面树的某一个检验类节点右击，在弹出的快捷菜单中选择“修改检验类”命令，会看到图 5-45 所示的“修改检验类详细信息”对话框。

修改完毕该检验类信息后单击“确定”按钮返回；单击“取消”按钮可取消修改操作。

或者在系统主界面中，选中右面列表中某一个检验类单击，然后单击列表下方检验类详细信息的“修改”按钮，就可以对该检验类进行修改，修改完毕后单击“确定”按钮即可保存。

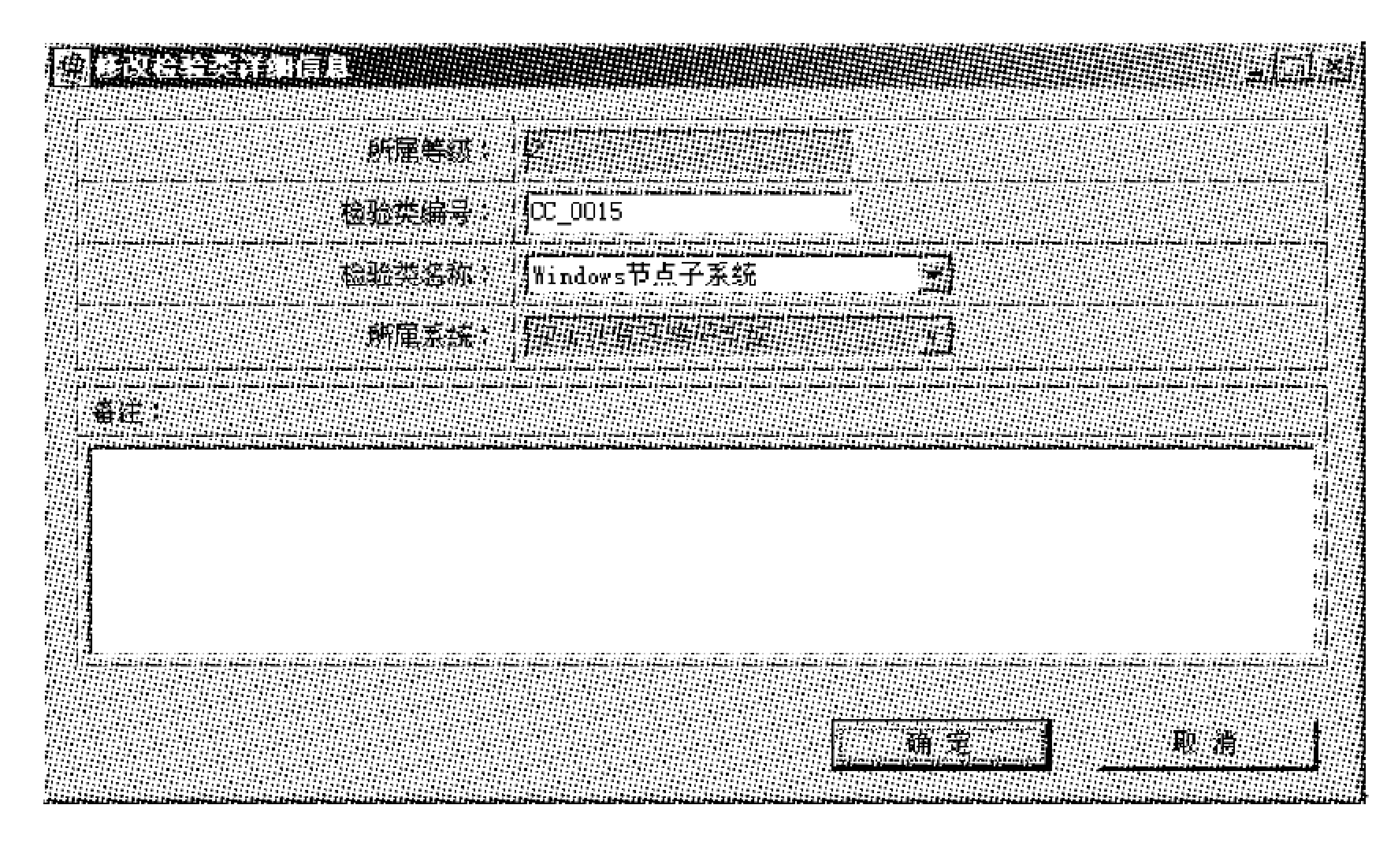



图 5-45 “修改检验类详细信息”对话框

## 4. 删除检验类

选中左面树的某一个检验类节点右击，在弹出的快捷菜单中选择“删除检验类”命令，或者选中右面列表中某一个检验类，然后右击，在弹出的快捷菜单中选择“删除检验类”命令，或者选中右面列表中某一个检验类，然后单击上面菜单中的“删除检验类”命令，在弹出的图 5-46 所示的“确认删除”对话框中单击“是”按钮删除被选中的检验类，或单击“否”取消删除操作。




图 5-46 “确认删除”对话框

# 第6章 信息安全风险评估工具的使用

## 6.1 体系结构

奥运信息网络安全风险评估系统为奥运相关网络及信息系统风险评估提供了支撑。信息系统由于安全威胁的存在和脆弱性不能及时得到弥补，总会存在这样或那样的安全隐患。风险评估旨在通过对系统关键资产各方面的评估，从安全威胁的可能性和影响两个方面分析系统的安全风险。

本系统以威胁来源为核心，通过威胁分析发现现有的安全威胁，在此基础上确定威胁所针对的脆弱性，进一步分析保护对象存在的脆弱性，明确威胁对保护对象造成的影响，从而实施风险评估工作。

根据对近期奥运相关风险评估的需求以及中远期针对行业的信息安全风险评估需求，该系统设计应该考虑到针对各类信息资产所特定面临威胁类别及其可被利用脆弱性的关系群集合所覆盖的各类风险要素。

对于风险要素资产、威胁、脆弱性的识别，可采用按类自动搜索、文档输入以及手动输入三种方式进行；资产重要性的赋值可按类根据其CIA属性及其所受影响计算；威胁赋值可根据各类资产所面临的具体威胁类别的历史故障统计或根据国际、国内发布的该类威胁的统计数据进行计算；脆弱性赋值可根据通用和专用的漏洞扫描结果进行赋值；三要素赋值均按照国家标准算法进行计算。奥运信息网络安全风险评估系统逻辑结构如图6-1所示。

该风险评估系统功能设计分为四个层次：用户接口层、数据处理层、数据存储层和数据获取层。

① 用户接口层由保护对象分析、威胁分析、脆弱性分析、已有控制措施分析、风险分析、风险处置、统计分析、项目管理以及系统管理等功能模块组成，人工、文档数据的输入处理也由该层的各相关功能模块实现。

② 数据处理层负责系统的管理和配置、风险要素的关联分析、智能分析和结果判定、结果提取及统计分析等功能。由于通过人工输入、表单获取和扫描工具等手段获取的数据格式不同，系统将在数据处理层提供统一的可供识别的数据格式来实现数据的合并处理。

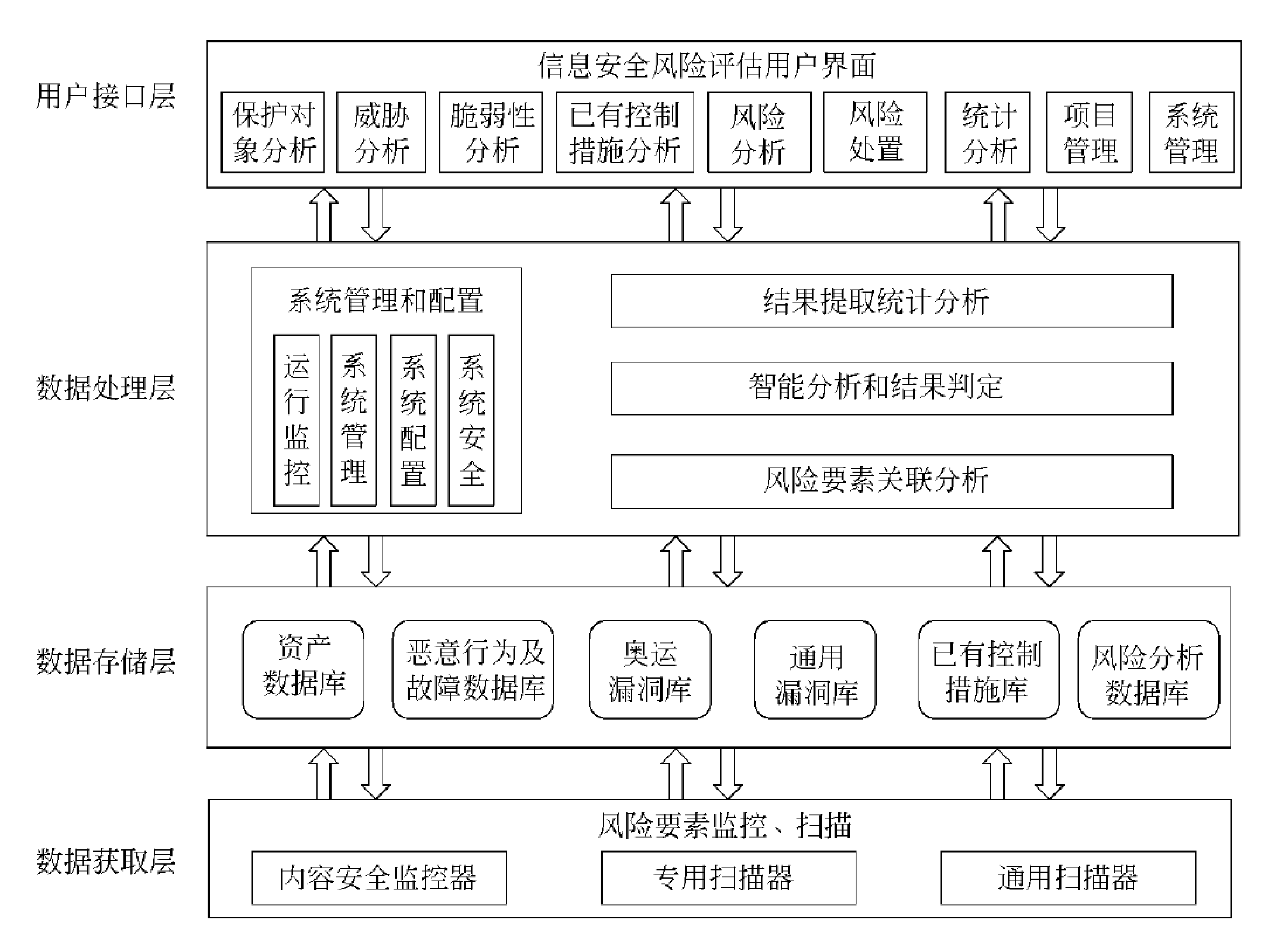



图 6-1 奥运信息网络安全风险评估系统逻辑结构

③ 数据获取层负责各类风险要素的识别、扫描分析，包含内容安全监控器、专用扫描器、通用扫描器等功能模块。其中：

- 内容安全监控器主要负责信息内容资产以及信息内容敏感数据（威胁因素）收集，所收集的信息分别存储在数据存储层的资产数据库和恶意行为及故障数据库中，以便用户接口层的调用分析。
- 专用扫描器主要负责奥运 Web 应用服务的漏洞扫描，存储在奥运漏洞数据库中，以便对照配合内容安全监控器搜集的资产类及威胁类数据的关联分析。
- 通用扫描器主要负责通用漏洞的扫描，其扫描数据按资产和脆弱性类别分别存储在数据存储层的资产数据库和通用脆弱性数据库中。

④ 数据存储层负责对六大类数据库的维护和管理，它们分别是：资产数据库、恶意行为及故障数据库、奥运漏洞库、通用漏洞库、已有控制措施库和风险分析数据库。这几类数据库除了从数据获取层的三大监控扫描工具中自动获取之外，在评估过程中还可以通过各类调研、调查数据、专业人员访谈等手段，在评估系统客户端经人工输入对各类数据进行补充修订，存储到相应的数据库中。已有措施控制库的数据主要来源于对被评估对象的实际调研，并通过人工输入的方式输入到数据库中。人工输入的方式有两种：一种是通过功能模块中对各类风险要素的编辑实现增加、删减、修改等的操作；另一种是按照特定的数据格式将所有已编辑好的各风险要素及其属性数据一次性读取到数据库中存储，实现批量处理。

# 6.2 功能结构

信息安全风险评估系统共有 12 个模块，分别为系统功能模块、类型管理模块、用户管理模块、项目管理模块、保护对象功能模块、威胁分析模块、脆弱性分析模块、控制措施有效性分析模块、风险分析模块、风险处置模块、统计分析模块和报告生成模块。其中保护对象分析模块又可细分为 4 个模块，分别为网络资产、软件及服务资产、信息及内容资产和人员资产。脆弱性分析模块也可细分为 3 个模块，分别为手工检查、管理核查和技术测试，如图 6-2 所示。

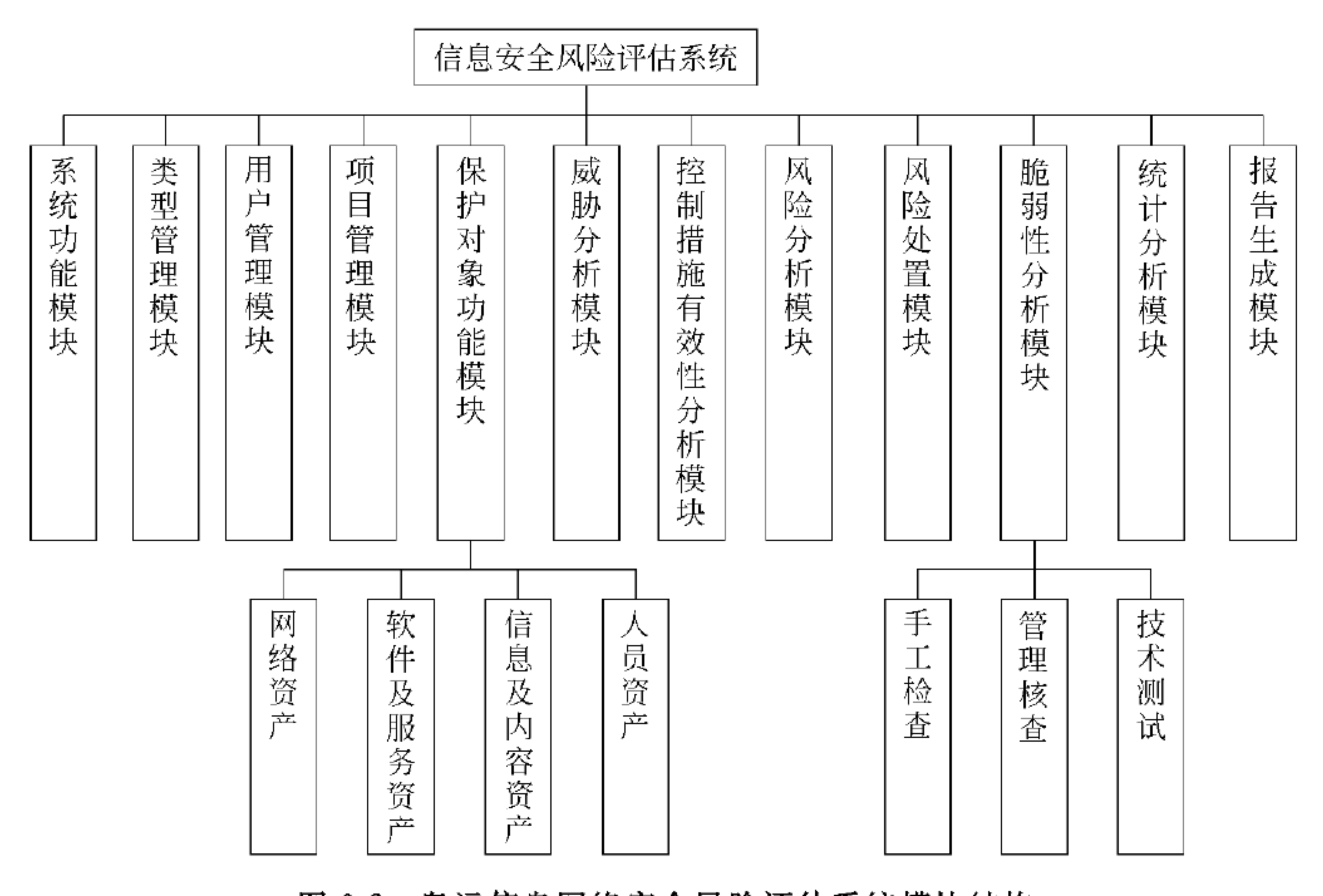



图 6-2 奥运信息网络安全风险评估系统模块结构

系统功能模块提供系统相关的访问控制功能，是综合分析平台安全的保证。类型管理模块包括风险分析过程中各相关分析因素的类型管理，属于分析平台整体设置的范畴。用户管理模块提供系统用户信息和权限管理功能，与访问控制功能相结合为综合分析平台运行提供了保证。保护对象分析、威胁分析、控制措施分析、脆弱性分析模块、风险分析以及风险处置模块提供了一个针对特定项目的完整风险评估和计算流程。统计分析模块则是针对上述各个阶段分析结果进行的数据统计和分析。

其中，威胁分析模块对外提供与内容监控器的接口，同时该模块后台需要恶意行为库的支撑方能完成最终的威胁分析。脆弱性分析模块的技术测试部分为通用扫描器提供了扫描结果的导入接口。

类型管理模块后台需要保护对象类型库、恶意行为库、脆弱性类型库和控制措施类型库的支持。为了实现以上的方便，在系统的设计中保护对象类型库、脆弱性类型库和控制措施类型库都以系统库中的相关数据表的方式实现。恶意行为库则作为一个单独的库存在。

# 6.3 设计与实现

## 6.3.1 系统权限设计

系统共设 5 类用户。其中可分为两个大类，即系统管理员和普通用户。普通用户又可分为项目经理、手工检查人员、管理核查人员、技术测试人员 4 类，如图 6-3 所示。

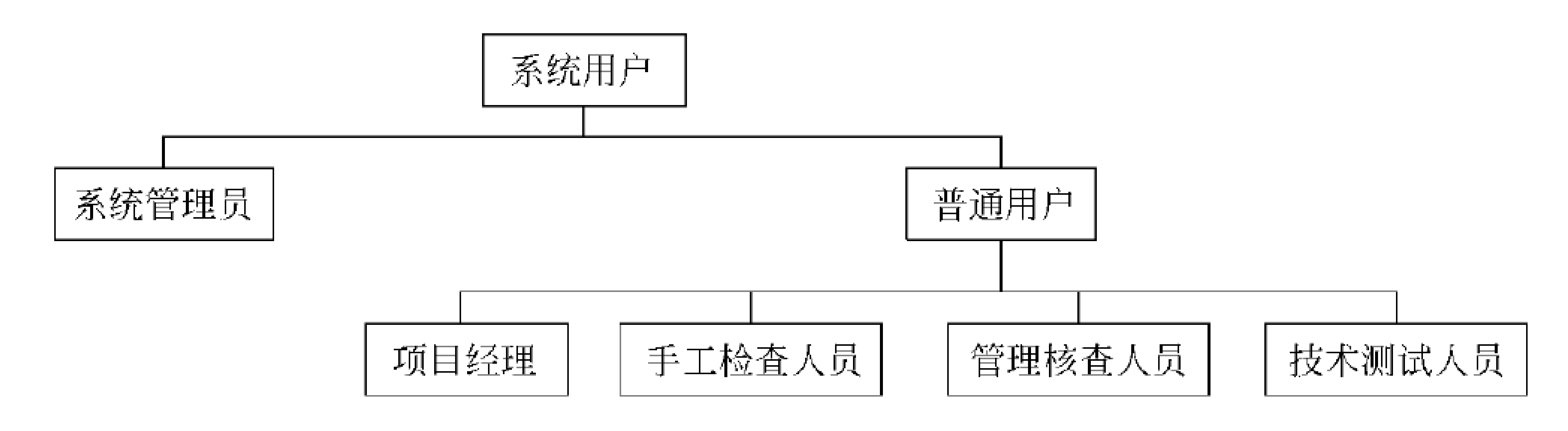



图 6-3 奥运信息网络安全风险评估系统的用户结构

系统管理员负责维护整个评估平台。系统管理员负责创建、删除评估项目，设定可访问 IP，添加、删除用户，指定项目的项目经理、管理核查人员和技术测试人员。

项目经理为所制定的项目负责。例如可以指定手工检查人员，填写项目信息，进行保护对象分析、威胁分析、脆弱性分析、控制措施有效性分析、风险分析、风险处置和统计分析等。

手工检查人员负责脆弱性分析中的手工检查，并进行手工检查测试表单答案的填写、修改和删除等工作。

管理核查人员负责脆弱性分析中的管理核查，并进行管理核查表单答案的填写、修改和删除等工作。

技术测试人员负责脆弱性分析中的技术测试，并进行扫描器和内容监控器的扫描和监控功能，然后将结果按固定格式保存成 XML 文档。

## 6.3.2 接口设计

### 1. 外部接口

奥运信息网络安全风险评估系统的外部接口主要是与扫描器和内容监控器的接口。两者之间的接口为 XML 格式的结果。扫描服务器对目标网络扫描完成以及内容监控器都会生成 XML 格式的结果，奥运信息网络安全风险评估系统可将扫描结果导入系统，如图 6-4 所示。

### 2. 用户接口

本系统为用户提供了易于操作的用户界面，用户要进行的各种操作通过在各个界面上单击或输入或提交就可以完成。对于该系统在运行过程中随时可能出现的各类提示信

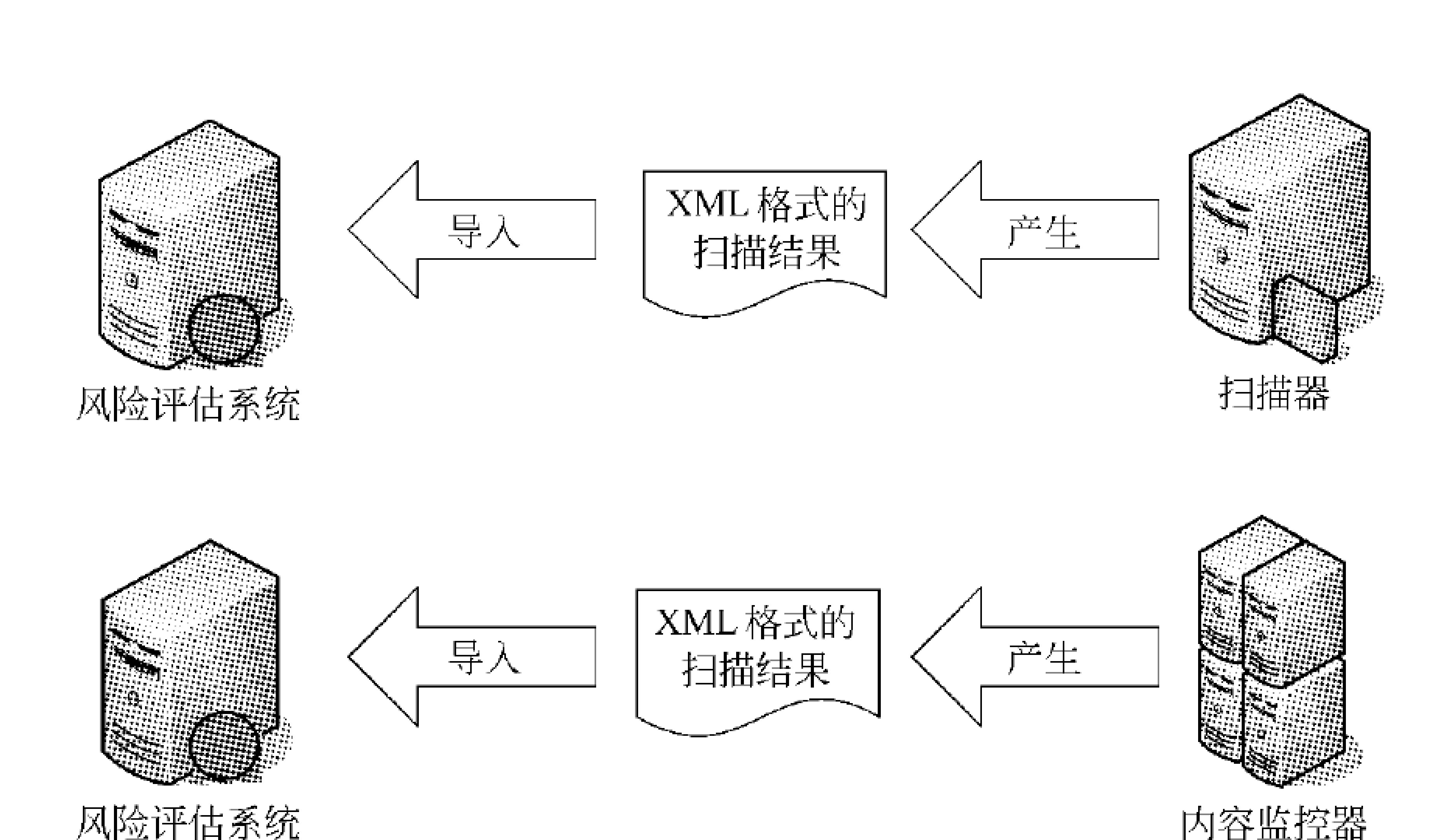



图 6-4　风险评估系统外部接口

息和警告信息，大多会用页面提示信息来显示。另外，基于系统安全的考虑，系统对用户权限有严格的控制，这样具有不同权限的用户可以进行的操作就不相同，用户不能使用的功能对用户来说是可见不可用。另外，由于测评流程有着严格的顺序限制，这样用户可见但不能进行操作也可能是因为当前项目还不具备进行该操作的数据。系统主界面，如图 6-5 所示。



图 6-5　登录界面

### 3. 内部接口

系统各模块之间通过数据库共享数据，因此系统内部接口的设计实际可以归结为系统数据库的设计。

### 6.3.3 数据结构设计

从逻辑上来说，风险评估涉及到的主要概念包括保护对象、威胁、系统信息、脆弱性、安全措施、风险等。在风险评估的实施过程中有可能会借助技术测试和管理核查等手段，有可能会涉及到测试表单和测试方法，以及问卷、问题和答案等。这些概念在系统的设计过程中都将与相应的类对应。类之间的逻辑关系设计如图 6-6 所示。此外，保护对象由于分为不同的类别，因此与其他类之间是父子的关系。具体类的继承关系如图 6-7 所示。

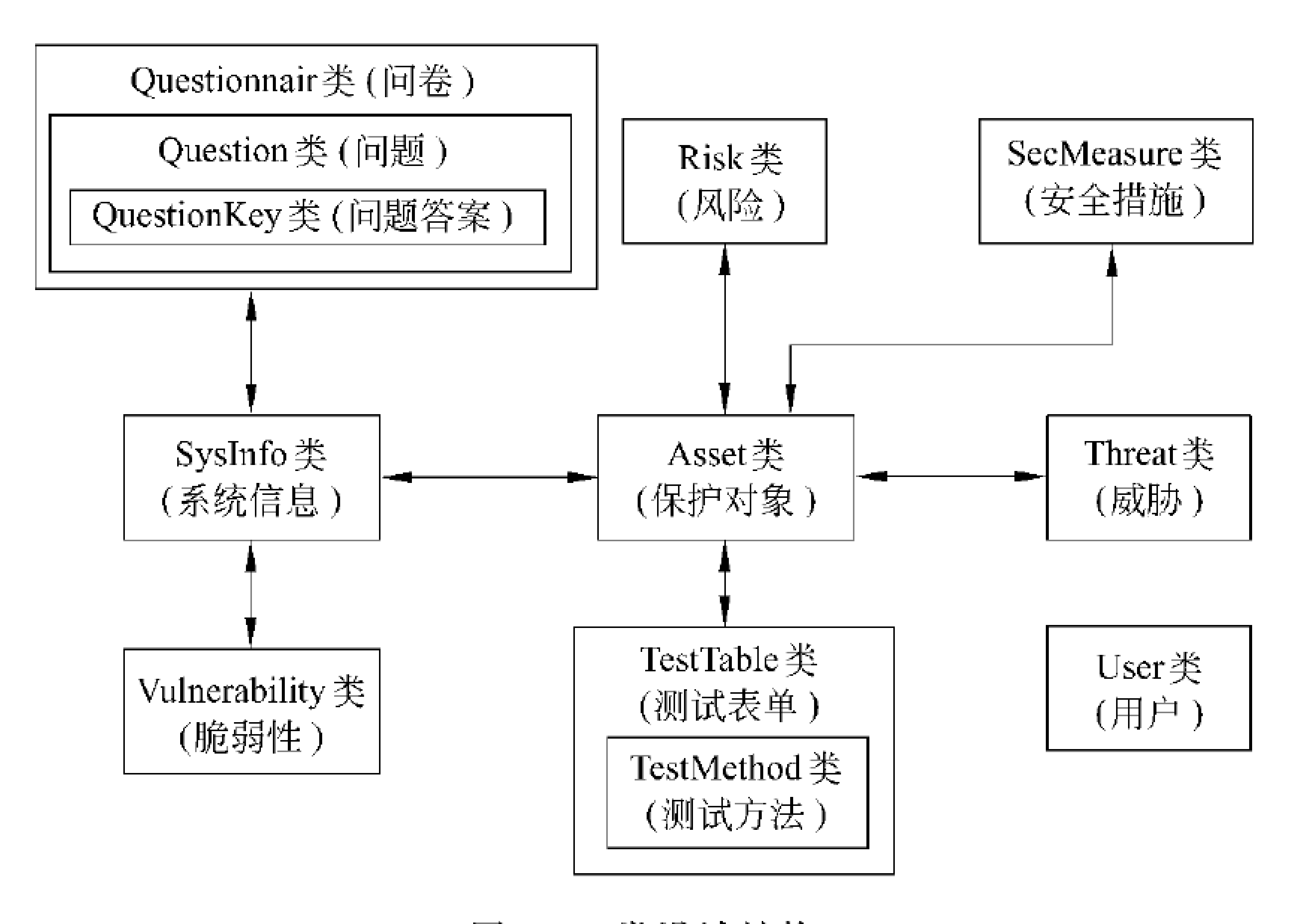



图 6-6　类设计结构

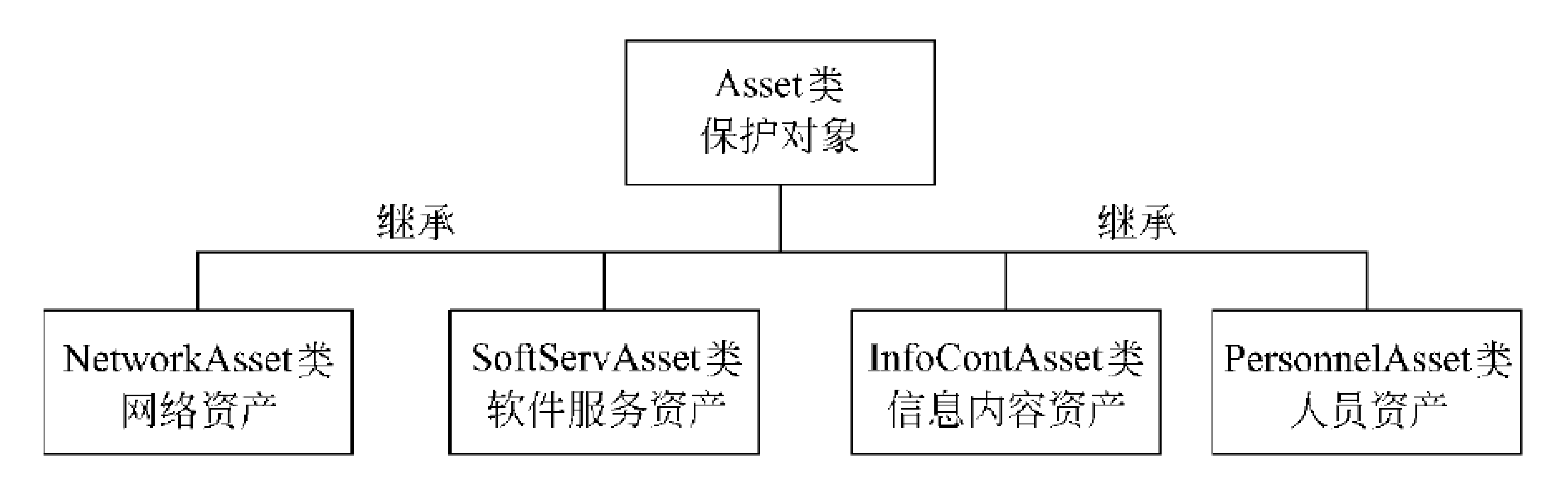
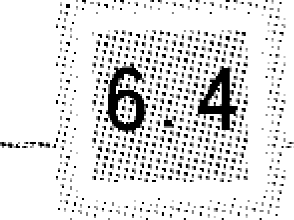



图 6-7　保护对象类的继承关系



## 6.4 使用操作演示

### 6.4.1 用户登录

配置好数据库和 IIS 之后，打开浏览器，在地址栏输入“http://localhost/oly-replat”，按回车键之后浏览器会进入用户登录界面。然后输入相应的用户名、密码、验证码之后就可以登录系统了。根据用户角色的不同，登录后的界面及可使用的功能会有所不同，主要

分为管理员角色功能模块和普通用户功能模块，下面将分别以这两种用户身份为例进行相应的操作演示。

## 6.4.2 系统管理员操作演示

### 1. 项目管理

用户以系统管理员身份登录后所显示的对话框就是项目管理对话框。用户还可以通过单击左侧“风险评估”链接进入项目管理。

(1) 新建项目

在主页面上单击“新建项目”按钮将进入新建项目界面，如图 6-8 所示。

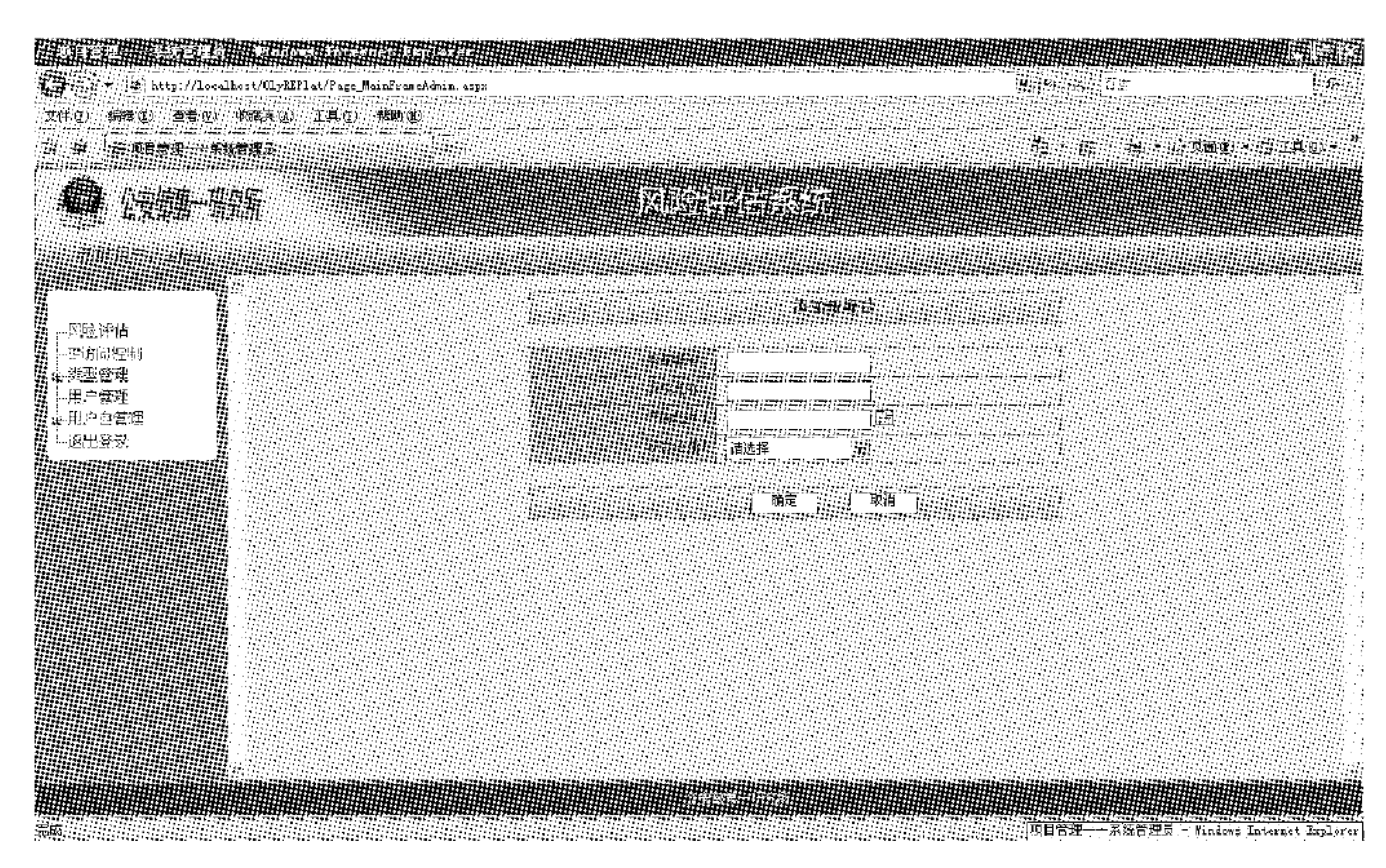



图 6-8 新建项目对话框

在页面中输入系统编号、系统名称、开始时间，并选定项目经理后单击“确定”按钮，即可生成一个新项目。单击“取消”按钮将返回。

输入项目开始时间可以利用页面中的日历控件选取。

(2) 删除项目

项目删除可以通过选择或者批量的方式进行删除。

选择方式删除方式是首先在对话框中选取一个或多个项目，单击“删除所选”按钮，页面跳转至确认删除对话框，单击“确认”按钮后删除所选项目信息。

批量方式删除方式首先在主界面中单击“删除所有”按钮，页面跳转至确认删除所有项目对话框，单击“确认”按钮后删除所有项目信息。

(3) 查看/修改项目

在主页面上单击项目的系统编号，将进入项目的查看对话框，如图 6-9 所示。在查看对话框单击“修改”按钮，将进入项目的修改对话框，修改完相应信息后单击“确定”按钮完成修改操作。

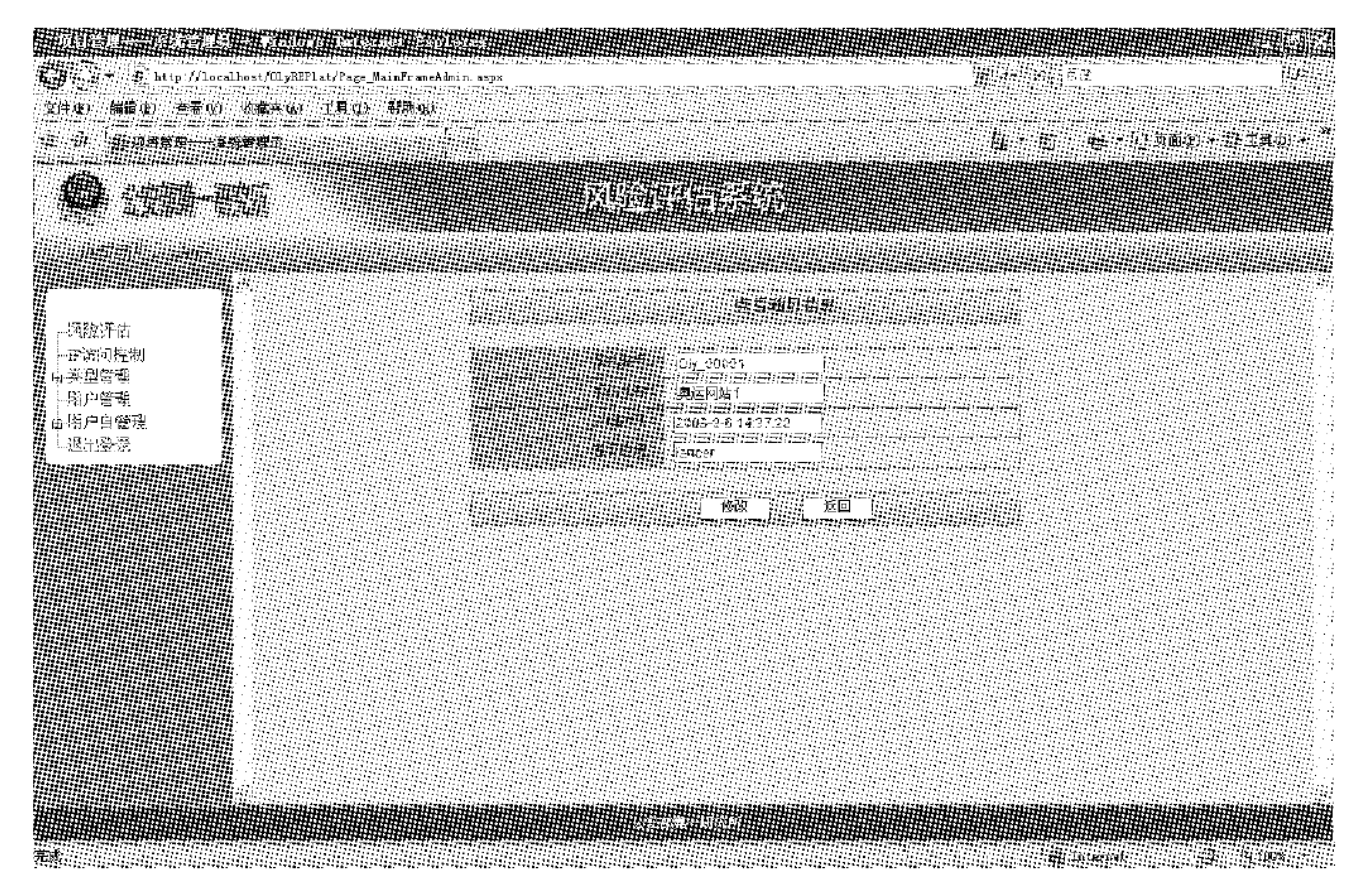


图 6-9 查看项目对话框

## 2. IP 访问控制

IP 访问控制是设置允许访问风险评估服务器的所有客户端的 IP 地址，只有添加在 IP 列表中的客户端才可以正常访问服务器，来进行风险评估的相关工作。

用户可以单击对话框左侧“IP 访问控制”链接进入 IP 访问控制管理模块，如图 6-10 所示。

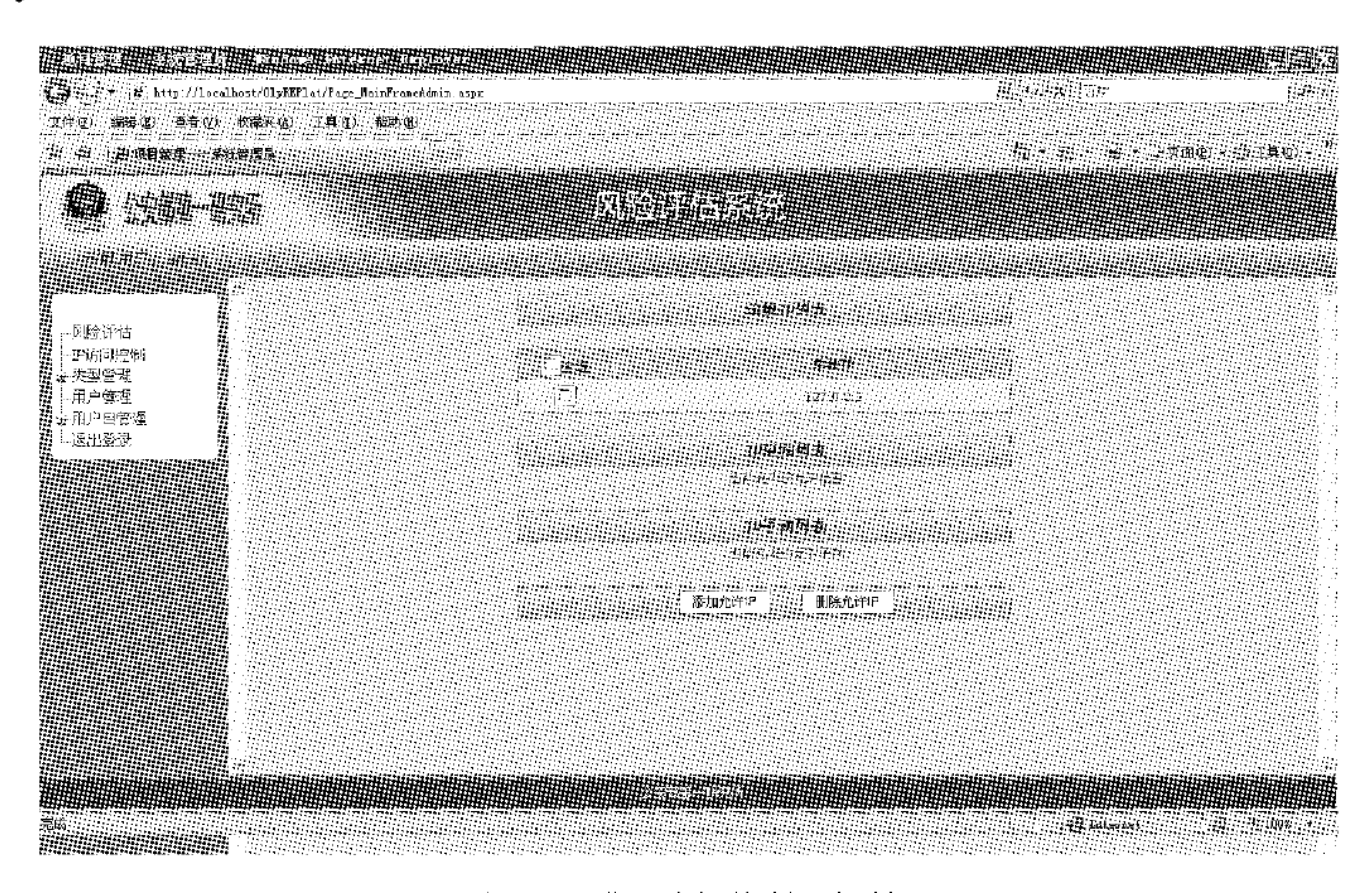


图 6-10 “IP 访问控制”对话框

(1) 添加可访问 IP

在 IP 访问控制页面中单击"添加允许 IP"按钮，进入添加 IP 对话框。在对话框中选择添加类别(单独 IP、IP 范围、子网)，然后单击"确定"按钮即可。单击"取消"按钮，返回 IP 访问控制对话框。

(2) 删除可访问 IP

在可访问 IP 对话框选中欲删除的 IP，单击"删除允许 IP"按钮。会出现确认删除对话框三。单击"确认"按钮即可删除。单击"取消"按钮返回可访问 IP 的对话框。

## 3. 用户管理

单击对话框左侧的"用户管理"链接进入"用户管理"对话框，在此可以进行用户信息的添加、修改和删除操作，如图 6-11 所示。




图 6-11　"用户管理"对话框

(1) 添加用户

单击用户管理页面中的"添加用户"按钮，进入用户添加对话框，在对话框中输入用户名、口令并选择用户类型(系统管理员、普通用户)，单击"确认"按钮即可保存。单击"取消"按钮返回用户管理对话框。

(2) 删除用户

在用户管理页面选择欲删除的用户，单击"删除选定"按钮，进入确认删除对话框。再次单击"确定"按钮后即可删除，单击"取消"按钮返回用户管理对话框。

在用户管理页面中单击"删除全部"按钮，进入删除全部用户确认对话框。单击"确认"按钮即可删除所有用户，单击"取消"按钮返回用户管理对话框。

(3) 查看/修改用户

在用户管理对话框，单击用户名，进入用户查看对话框，如图 6-12 所示。在此对话框可查看用户的各项信息(密码除外)。

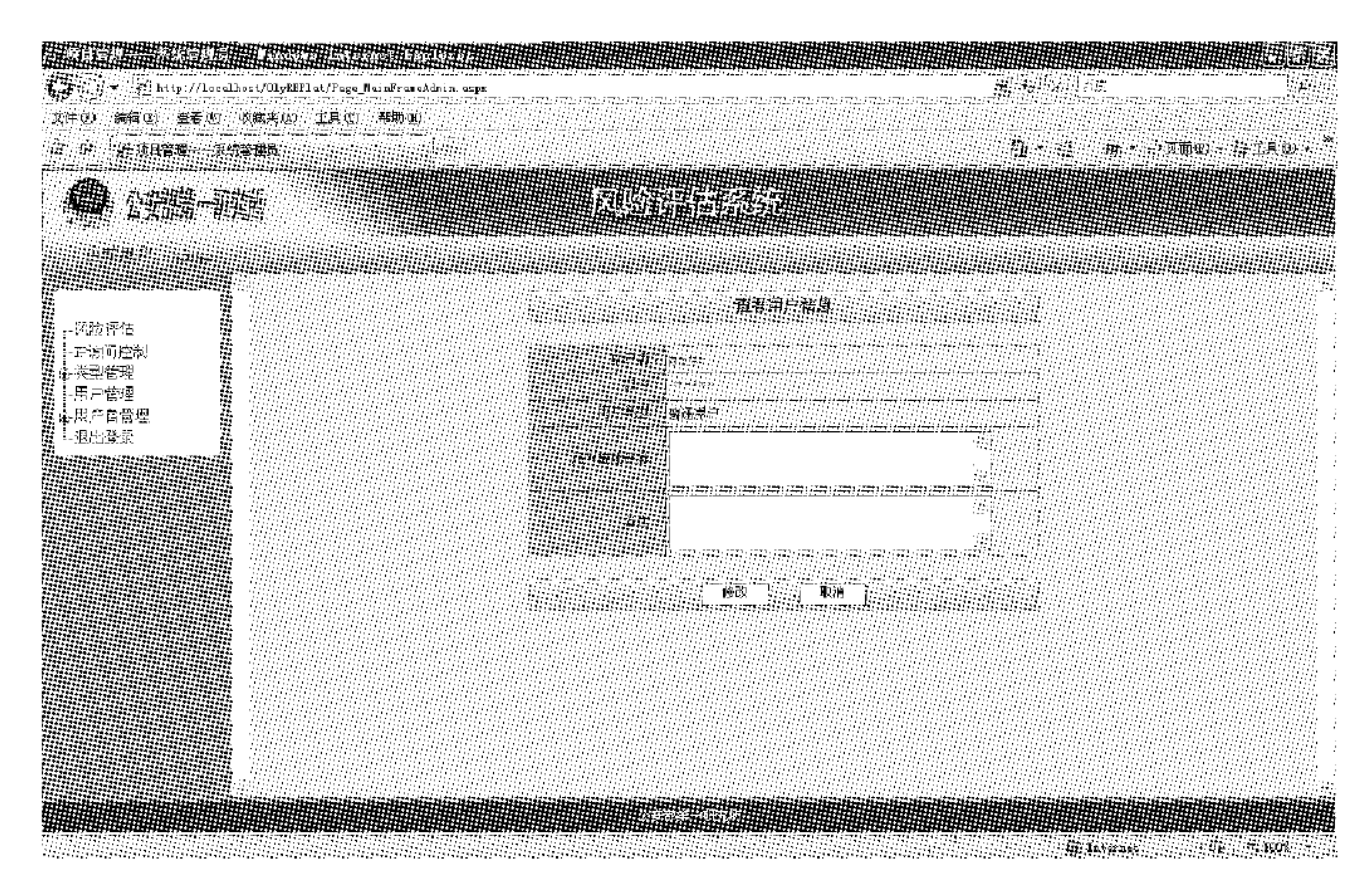


图 6-12 查看用户对话框

在查看用户对话框中单击“修改”按钮，即可进入修改用户对话框。在此对话框可以修改用户的各项信息，包括密码(需要知道旧密码)。

修改完成后，单击“确定”按钮即可完成保存，单击“取消”按钮返回用户管理页面。

#### 4. 用户自管理

单击主页面左侧“用户自管理”链接，会出现两个子选项：修改口令和修改用户信息，可以对系统管理员自身的信息进行修改。

(1) 修改口令

单击“修改口令”链接进入口令修改对话框。输入该用户的旧密码和欲改成的新密码后，单击“确定”按钮即可。单击“取消”按钮出现操作取消对话框。

(2) 修改用户信息

单击左侧“修改用户信息”链接进入用户信息修改对话框。在此对话框可修改用户信息和备注两项，不可修改用户类型、用户名等内容。

### 6.4.3 普通用户操作演示

在用户登录页面中以普通用户身份登录后，可以进行风险评估的具体操作流程。一次完整的风险评估流程包含威胁分析、保护对象分析、脆弱性分析、控制措施有效性分析、风险分析、风险处置、统计分析以及生成评估报告。同时普通用户还可以对当前负责的项目信息进行管理。

#### 1. 项目管理

(1) 查看项目信息

在主页面中单击想要查看的项目的编号，或者展开左侧风险评估链接，单击其中想要

查看的项目名称，将进入项目信息查看页面，如图 6-13 所示。单击页面中的“查看网络拓扑图”链接可在弹出窗口中查看已经上传的项目的网络拓扑图。

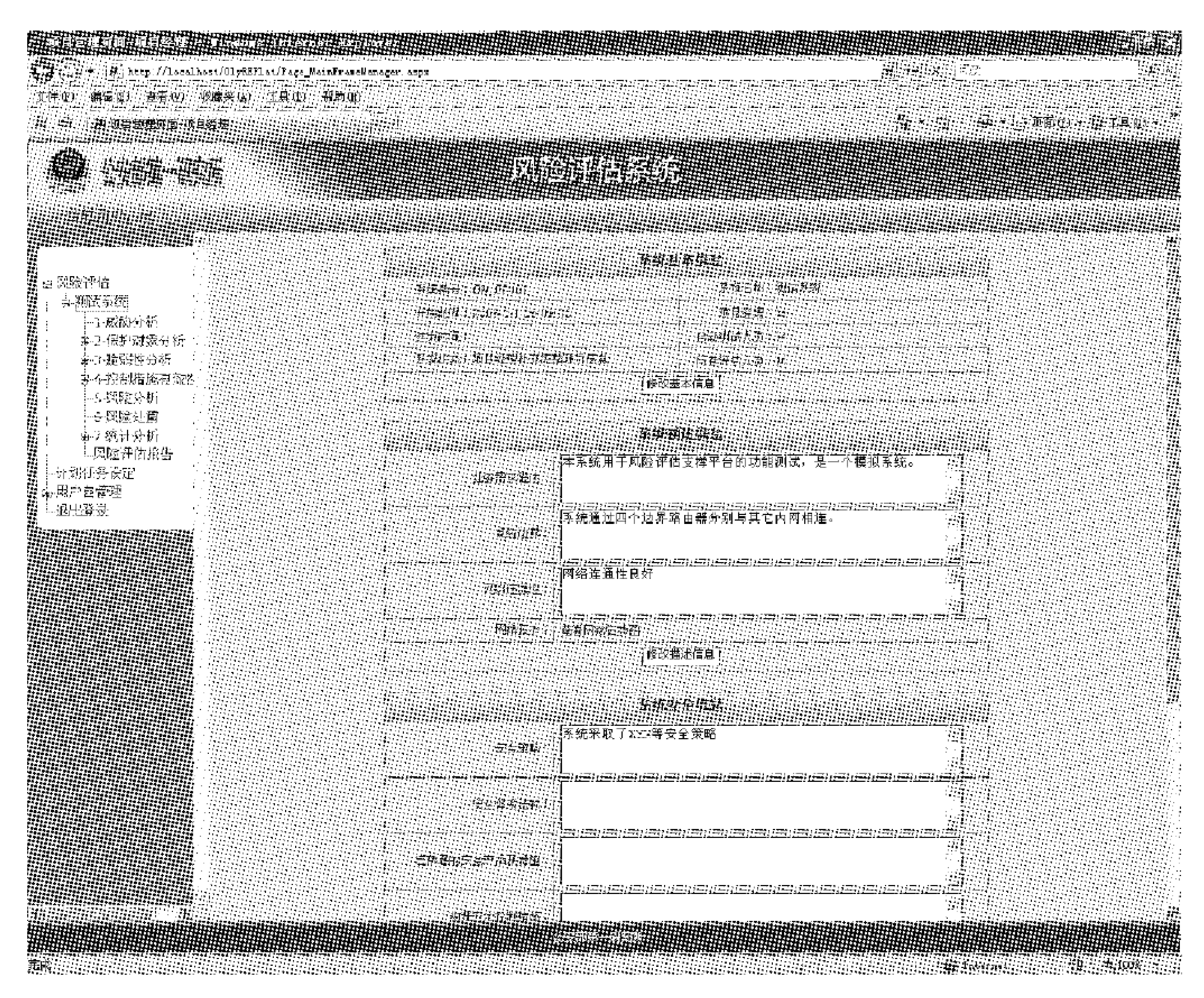



图 6-13　项目信息查看对话框

(2) 修改项目信息

① 基本信息

在项目信息查看对话框中，单击“修改基本信息”按钮，即可进入项目基本信息修改对话框，如图 6-14 所示。在此对话框中，可以对项目的系统编号、系统名称、开始时间、结束时间、自动测试人员、问卷评估人员、系统状态进行重新设定。

② 描述信息

在项目信息查看页面中，单击“修改描述信息”按钮，即可进入项目描述信息修改对话框。在此对话框中，可以对项目的业务描述需求、系统边界、网络连通性进行修改，并可以重新上传网络拓扑图(会覆盖掉原来的拓扑图)。

③ 安全信息

在项目信息查看对话框中，单击“修改安全信息”按钮，即可进入项目安全信息修改对话框。在此对话框中，可以对项目的安全策略、安全体系结构、已部署的安全产品及措施、物理安全控制措施、环境安全措施进行修改。

④ 其他信息

在项目信息查看页面中，单击“修改其他信息”按钮，即可进入项目其他信息的修改对话框。在此对话框中可以对项目的备注信息进行修改。

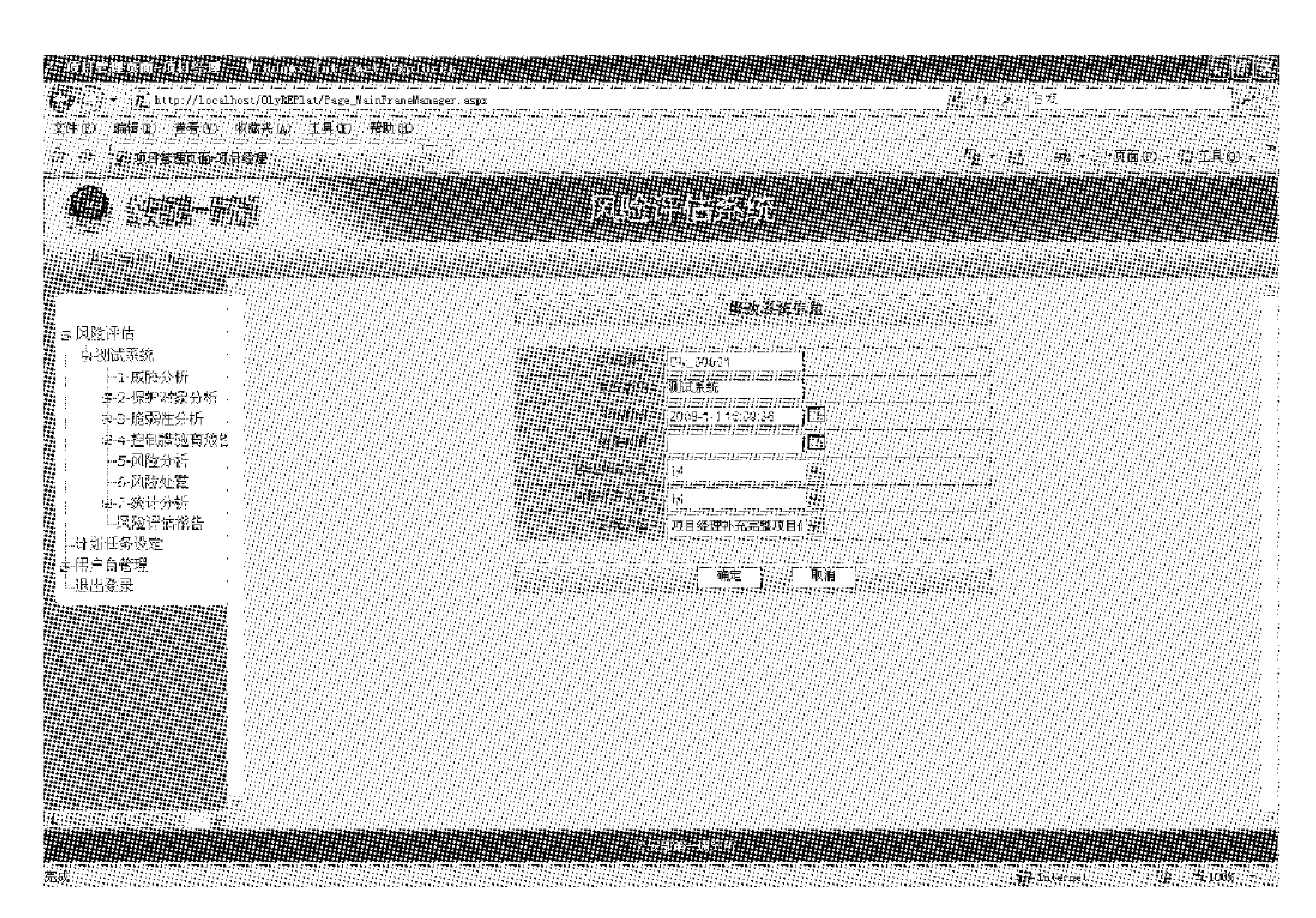



图 6-14　项目基本信息修改对话框

## 2. 威胁分析

单击左侧对应项目下的“威胁分析”链接，即可进入“威胁分析”对话框，如图 6-15 所示。此对话框可以进行威胁的增加、导入、删除、修改和威胁级别的计算等操作。

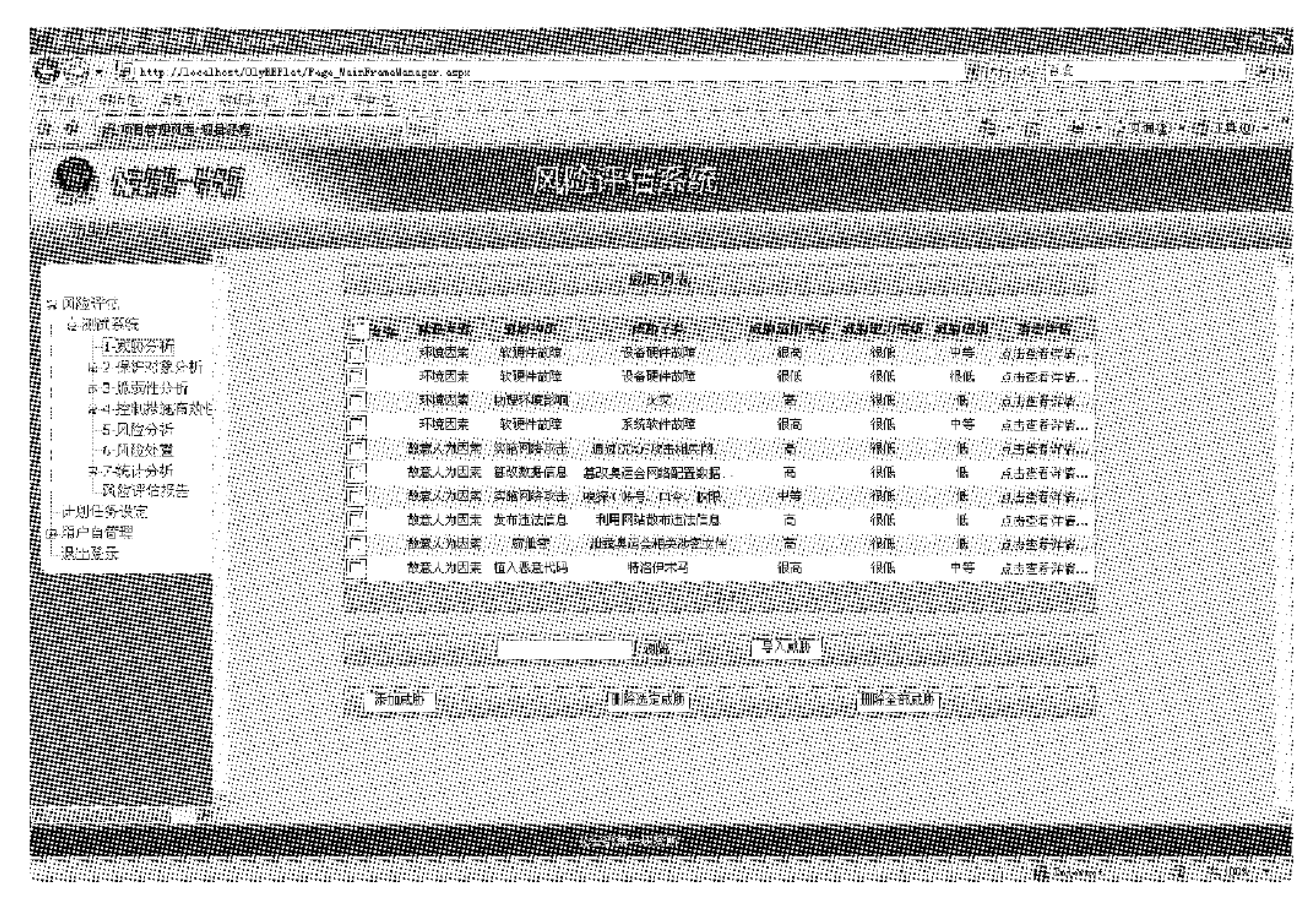



图 6-15　“威胁分析”对话框

(1) 添加威胁

在威胁分析对话框中单击“添加威胁”按钮即可进入威胁添加界面。本系统提供两种方式进行威胁的添加，分别是向导添加和快速添加。

① 向导添加

在威胁添加对话框左侧单击“进入向导添加页面”链接即可进行向导添加。向导添加通过七个步骤，引导使用者进行新添加威胁信息的设定。使用向导添加威胁时，前三个步骤是必需的，后四个步骤的内容可以不填。

每个步骤的具体内容依次分别为：设定威胁的来源信息、设定威胁的意图、设定威胁的能力等级、填写威胁的活动范围信息(此时已是选填内容，因此可以不填内容。同时，可以单击下方“完成”按钮，直接完成威胁的添加)、填写威胁的活动方式信息、添加威胁的活动方式信息和添加威胁备注信息。

② 快速添加

在威胁添加对话框左侧单击“进入快速添加页面”链接即可进入快速添加对话框。在此对话框中，一次性添加所有需要的威胁信息。其中，带红色星号的是必填信息，其余的是选填信息。

(2) 删除威胁

在威胁分析对话框中选中欲删除的威胁，然后单击“删除选定威胁”按钮会弹出确认删除对话框。单击“确定”按钮，则删除所选威胁；单击“取消”按钮，则返回威胁分析对话框。

在威胁分析对话框中单击“删除全部威胁”按钮，则进入删除全部威胁的确认对话框。单击“确定”按钮则确认删除所有威胁，单击“取消”按钮则返回威胁分析主页面。

(3) 查看/修改威胁

在威胁分析对话框中，单击相应威胁后面的“单击查看详情...”链接，即可进入查看威胁对话框，如图 6-16 所示。在此对话框中可查看威胁各种信息。继续单击“修改”按钮，即可进入修改威胁对话框。此对话框可以对威胁各项信息进行修改。修改完毕后单击“保存”按钮即可保存新修改后的内容，单击“取消”按钮则返回威胁分析对话框。

(4) 导入威胁

本系统支持 XML 文件格式导入威胁。在威胁分析对话框中单击“浏览”按钮，在弹出的对话框中的本地机器上选择待导入的 XML 文件。然后单击“导入威胁”按钮即可将 XML 文件中记录的威胁导入到系统中。

导入的威胁默认其威胁能力等级为很低，如需改变请手动更改。

### 3. 保护对象分析

保护对象可分为四类，网络类、软件及服务类、信息内容类和人员类。分别对应保护对象链接下面的四个子链接。

单击“保护对象”链接即可进入保护对象分析对话框，如图 6-17 所示。

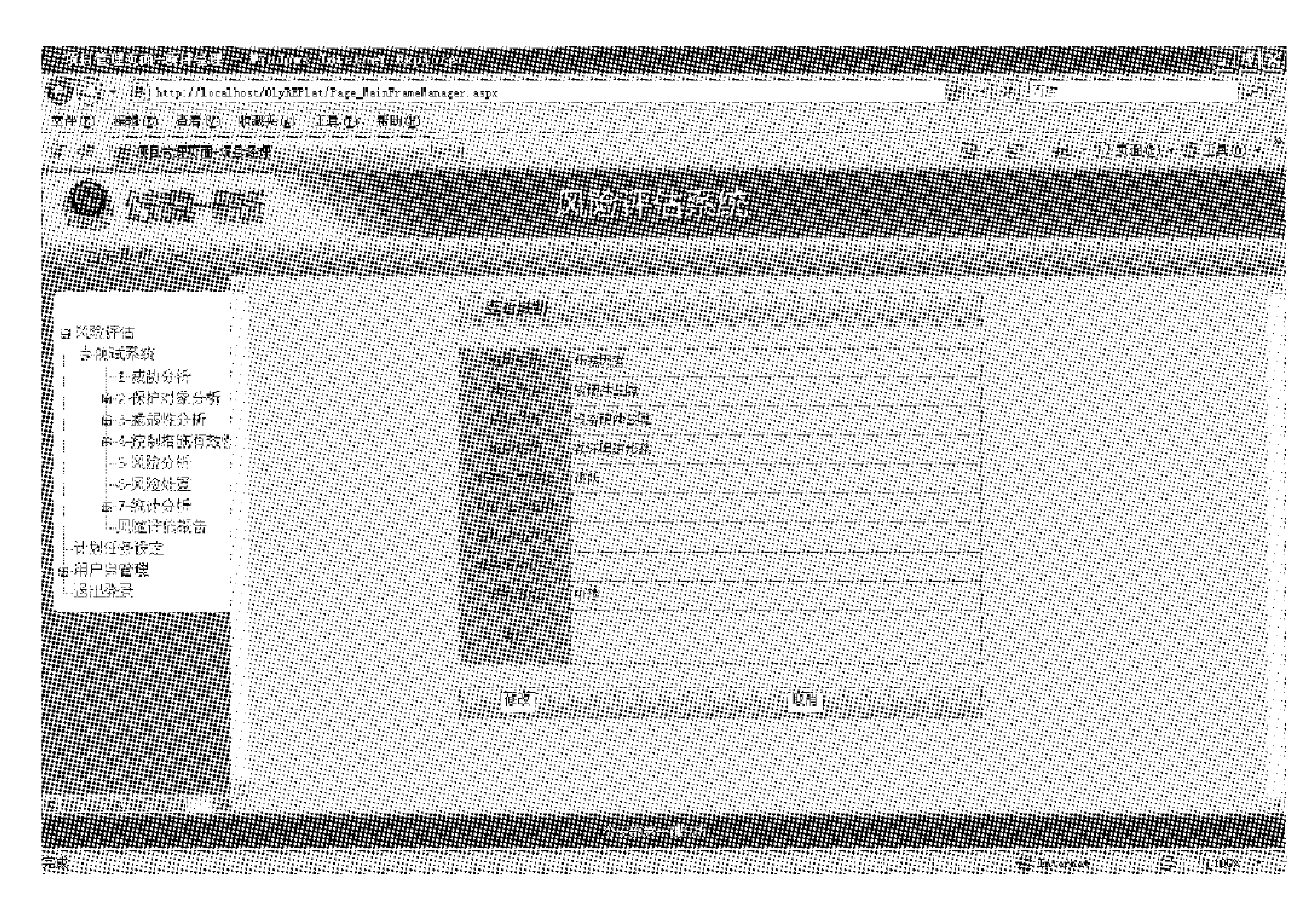



图 6-16　查看威胁对话框




图 6-17　保护对象分析对话框

(1) 添加保护对象

在保护对象分析对话框中单击“添加保护对象”按钮，即可进入保护对象添加对话框，如图 6-18 所示。在各栏填入或者选择相应的内容，单击“确认”按钮即可完成添加。单击“取消”按钮返回。

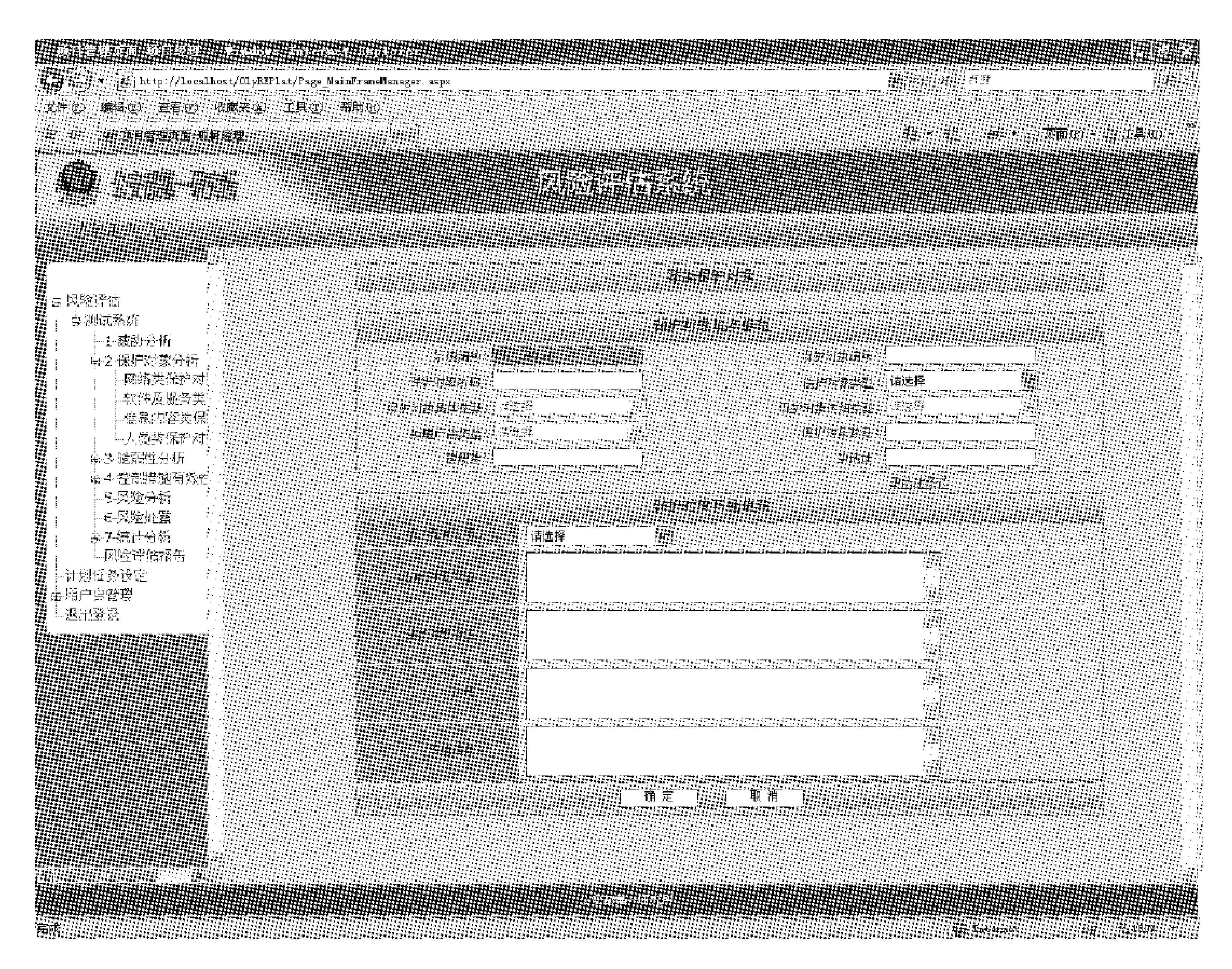


图 6-18　保护对象添加对话框

(2) 删除保护对象

在保护对象分析对话框中，选中欲删除的保护对象，单击"删除选定"按钮，将进入保护对象删除确认对话框。在此对话框中单击"确认"按钮完成删除，单击"取消"按钮返回保护对象分析对话框。

在保护对象分析对话框中，单击"删除全部"按钮，将进入删除全部保护对象确认对话框。在此对话框，单击"确认"按钮完成删除，单击"取消"按钮返回。

(3) 查看/修改保护对象

在保护对象分析对话框，单击保护对象编号可进入相应保护对象信息查看对话框。在此对话框可以查看保护对象的基本信息、价值信息和其他信息。

在保护对象信息查看对话框中单击"修改基本信息"按钮可进入保护对象基本信息修改。

在保护对象信息查看对话框中单击"修改价值信息"按钮可进入保护对象价值信息修改对话框，如图 6-19 所示。在此对话框中将对保护对象的完整性价值、可用性价值、机密性价值进行设定。同时还将设定保护对象这三类价值在总体价值中的权重，并可选择是否使用默认权重。另外，单击页面中的"单击查看详细帮助信息"链接将弹出新窗口，里面详细介绍了各项价值如何取值。

在保护对象信息查看对话框中单击"修改其他信息"按钮，将进入保护对象其他信息修改对话框。

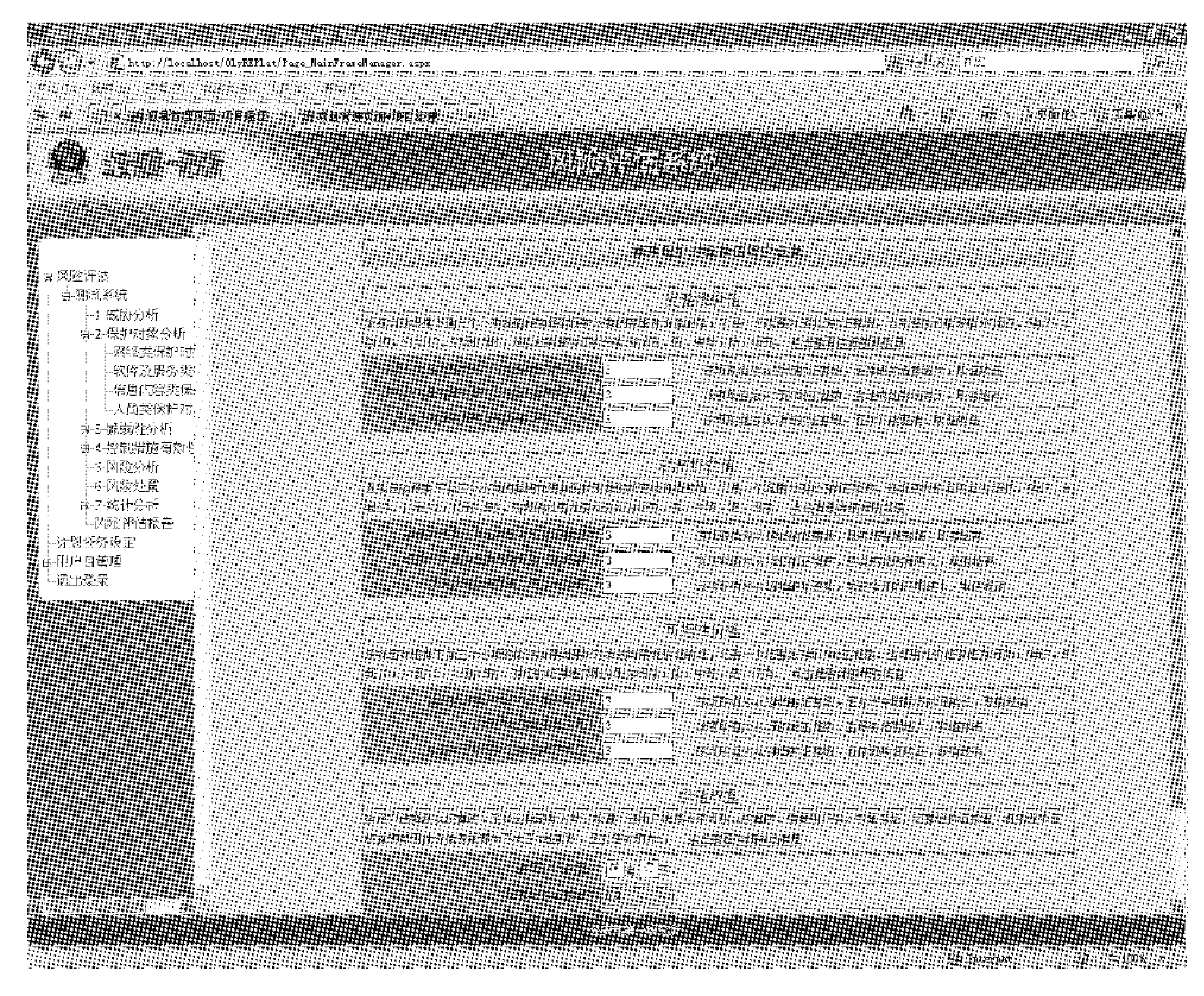


图 6-19　保护对象价值信息修改对话框

(4) 保护对象分类操作

在保护对象分析链接下有四个子链接，如图 6-20 所示。单击后可针对某一类保护对象进行操作。操作方法与上面介绍的相同。

-2-保护对象分析
  网络类保护对象
  软件及服务类保护对象
  信息内容类保护对象
  人员类保护对象
+3-脆弱性分析

图 6-20　保护对象分析及其子链接

## 4. 脆弱性分析

脆弱性测试分为两类，分别是技术测试和管理核查。

(1) 技术测试

技术测试包括两部分，手工检查和扫描结果导入。手工检查是通过问卷的形式对设备等进行技术上的配置检查从而识别出设备中的脆弱点。扫描结果导入是将扫描器扫描的结果导入到系统中。

① 手工检查

在对话框左侧依次单击“脆弱性分析”链接、“技术测试”链接、“手工检查”链接，将进入手工检查对话框，如图 6-21 所示。使用者可以通过对话框上方的下拉菜单选择欲检查的保护对象，并按照对话框提供的问题和步骤去考量。同时，使用者可以通过“导出安全检查操作手册”和“导出安全评估表”两个按钮将手工检查文件导出为 Word 文档，进而打印使用。当后台标准库修改后，可以通过“生成新的表单”按钮重新生成表单。

② 扫描结果导入及查看

单击左侧“扫描结果导入”链接，将进入扫描结果导入及查看对话框，如图 6-22 所示。在此对话框中可以导入并查看自动测试人员通过扫描器获得的脆弱性。

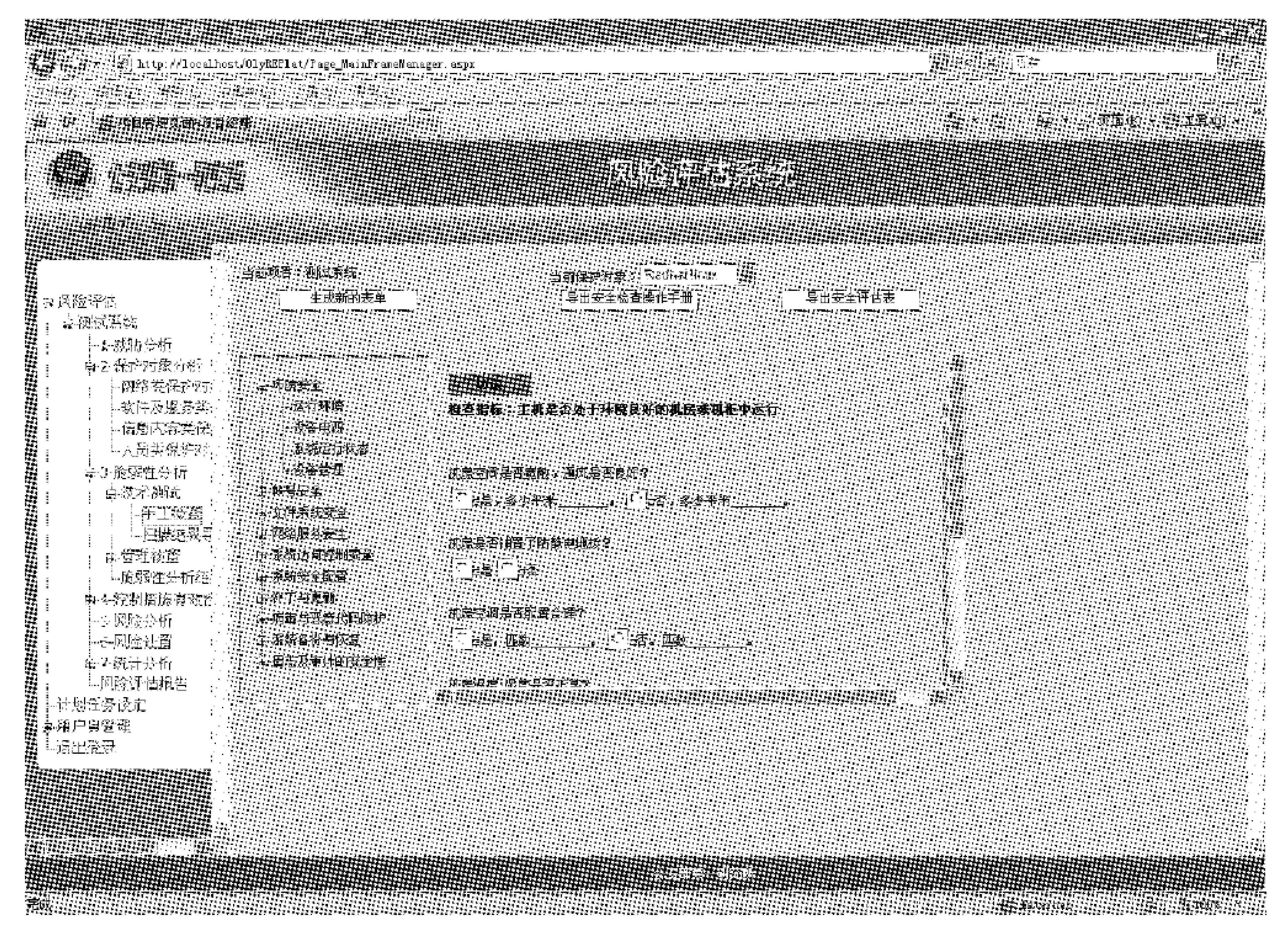



图 6-21　“手工检查”对话框




图 6-22　扫描结果查看对话框

在此对话框中，单击“浏览”选择待导入的 XML 文件，再单击“导入扫描结果”按钮，将显示导入对话框。选择想要导入的主机，单击“导入”按钮即可导入，单击“取消”按钮返回扫描结果查看对话框。

在扫描结果查看对话框中单击某一脆弱性的"查看"链接可以查看该脆弱性的详情。

(2) 管理核查

管理核查包括两部分,问卷的生成和查看。项目经理有权限查看问卷,问卷管理人员可以进行问卷的生成、删除和修改。

① 生成问卷

风险评估人员进行管理核查前需要先生成调查问卷,而要生成调查问卷必须以问卷评估人员的身份登录系统,而且生成问卷所属项目中的基本信息中"问卷评估人员"选项必须为当前登录用户。

具体的问卷生成操作流程请参考管理核查人员操作演示部分的内容。

② 查看问卷

单击对话框左侧的"查看问卷"链接,进入问卷查看对话框,如图 6-23 所示。



图 6-23 "查看问卷"对话框

(3) 脆弱性分析结果管理

单击对话框左侧"脆弱性分析结果管理"链接进入脆弱性分析结果管理对话框,如图 6-24 所示。在此对话框中可以查看经过技术测试后得到的技术类脆弱性,同时可以添加、修改在查看过管理核查问卷后发现的管理类脆弱性。

① 新建脆弱性

在"脆弱性分析结果"对话框中单击"新建"按钮可以新建管理脆弱性,如图 6-25 所示。其中带红色型号的项是必填项。新建脆弱性信息时,在"影响的保护对象类"选项中填写的内容一定是在"保护对象分析"中已经存在的信息,在"对应的威胁"选项中填写的内容一定是在"威胁分析"中已经存在的威胁信息,只有这样,所添加的脆弱性、保护对象以及威胁才能互相关联,后续的风险分析中才能得出正确的计算结果。




图 6-24　“脆弱性分析结果”对话框

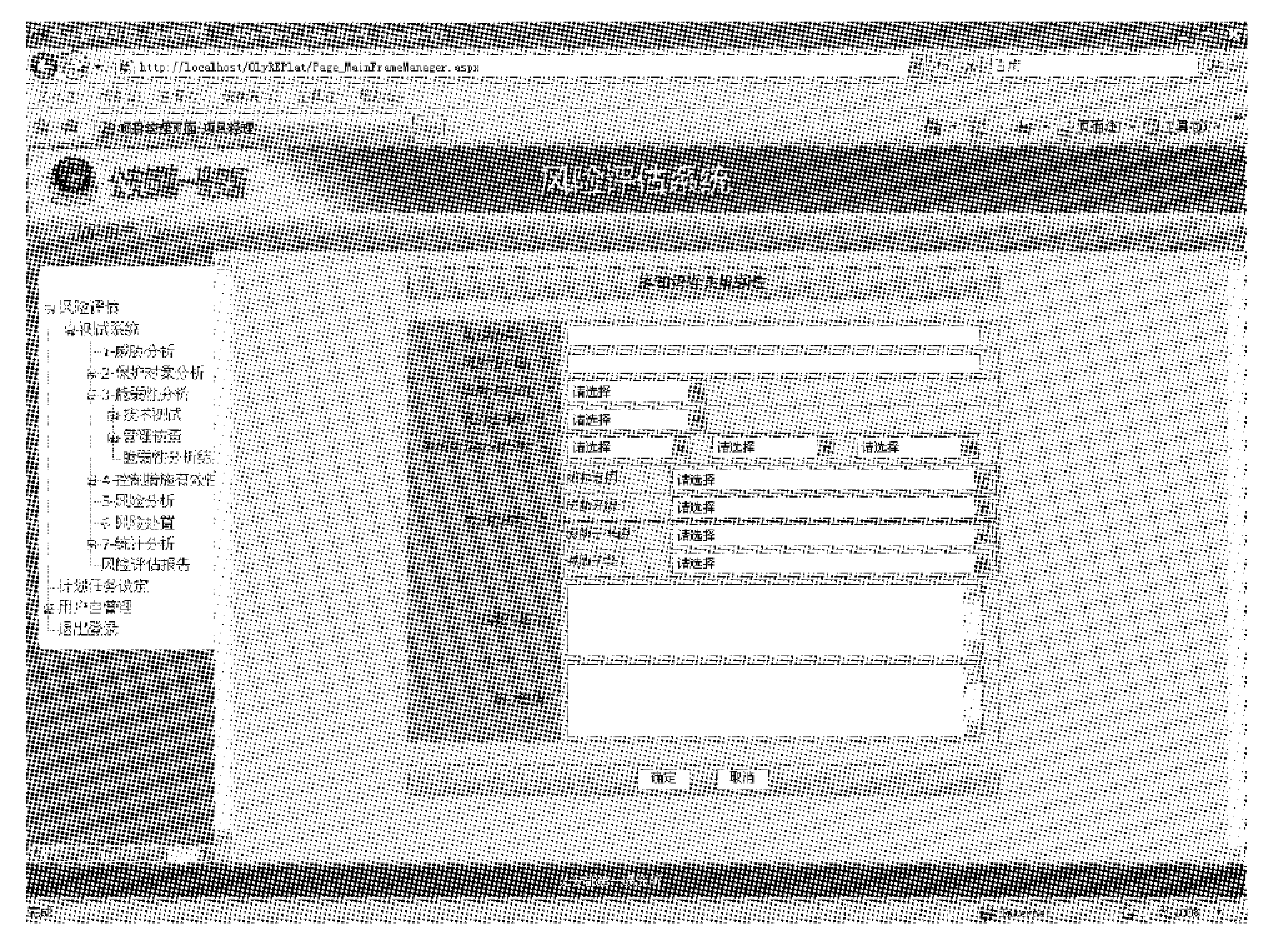



图 6-25　“添加管理脆弱性”对话框

② 查看与修改

在脆弱性分析结果管理对话框左侧，单击某脆弱性的“查看”链接可以进入该脆弱性的查看对话框，如图 6-26 所示。




图 6-26 “查看脆弱性”对话框

在脆弱性分析结果管理对话框中单击某管理类脆弱性的“编辑”链接，可以对该管理类脆弱性进行修改。但是对于技术类脆弱性不能进行修改。

③ 删除脆弱性

在脆弱性分析结果管理对话框中，选中欲删除的脆弱性，单击“删除选定”按钮，此时弹出确认删除对话框，如图 6-27 所示。单击“取消”按钮返回脆弱性分析结果管理对话

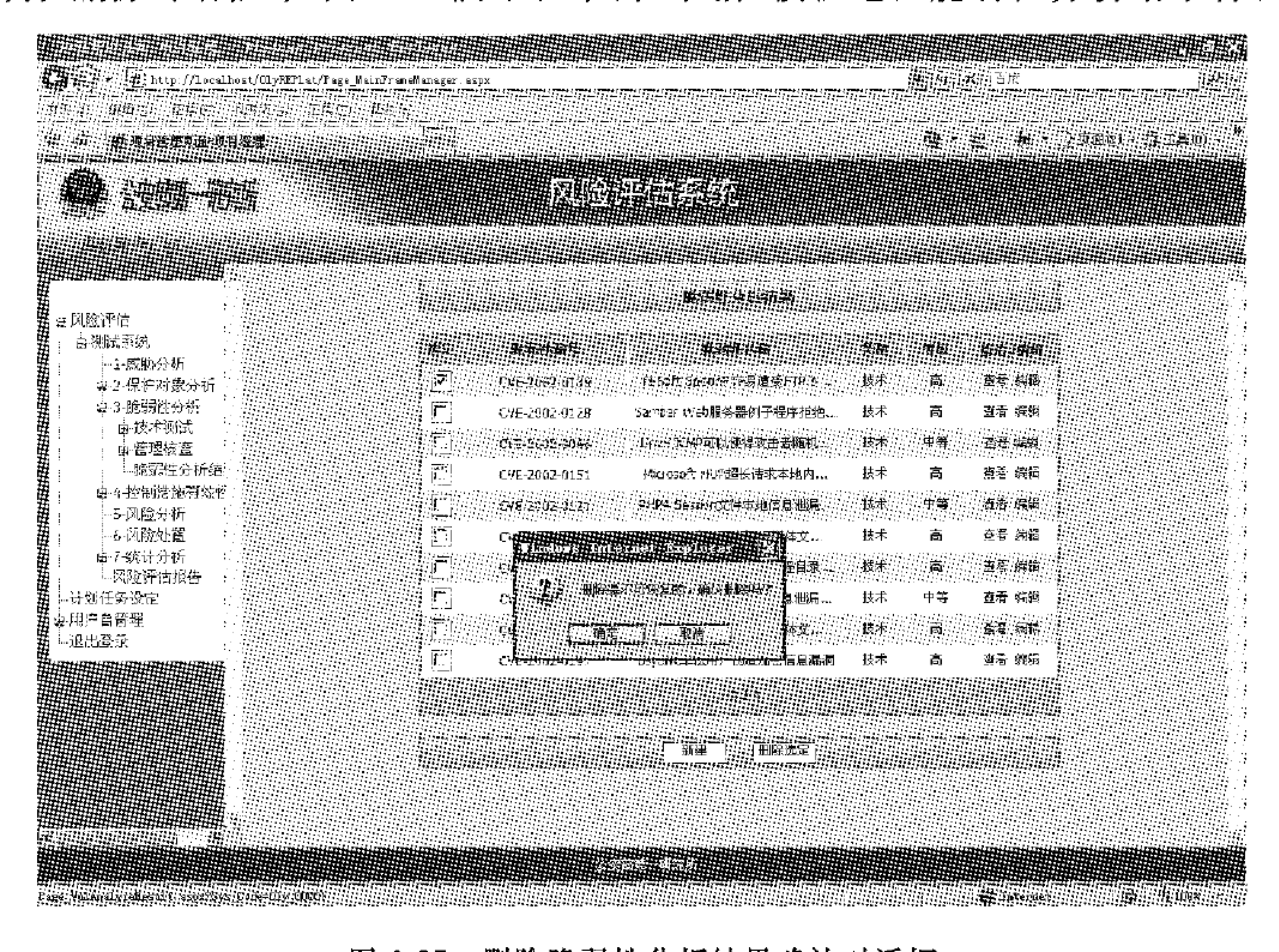



图 6-27 删除脆弱性分析结果确认对话框

框。单击“确认”按钮，若未选取，则弹出对话框提示未选取脆弱性分析结果，若选取的是技术脆弱性，则弹出对话框提示技术脆弱性不能删除，若选取的是管理类脆弱性，则可进行删除。

### 5. 控制措施有效性分析

单击左侧“控制措施有效性分析”链接，进入“控制措施有效性分析”对话框，如图 6-28 所示。




图 6-28　“控制措施有效性分析”对话框

(1) 添加控制措施

单击“添加措施”按钮，进入控制措施添加对话框，如图 6-29 所示。其中控制措施的名称、类型及有效性程度是必选项。填写完成后单击“确定”按钮完成添加。

(2) 查看与修改

在控制措施有效性分析对话框中，单击欲修改的控制措施的名称，进入控制措施查看对话框，如图 6-30 所示。在查看对话框中单击“修改”按钮，进入修改对话框。修改完成后单击“确定”按钮完成修改。

(3) 删除控制措施

在控制措施有效性分析对话框中，选择欲删除的控制措施，单击“删除选定”按钮，进入确认删除对话框，单击“确认”按钮完成删除。

在控制措施有效性分析对话框中，单击“删除全部”按钮，进入确认删除全部措施对话框，单击“确认”按钮完成删除所有控制措施。

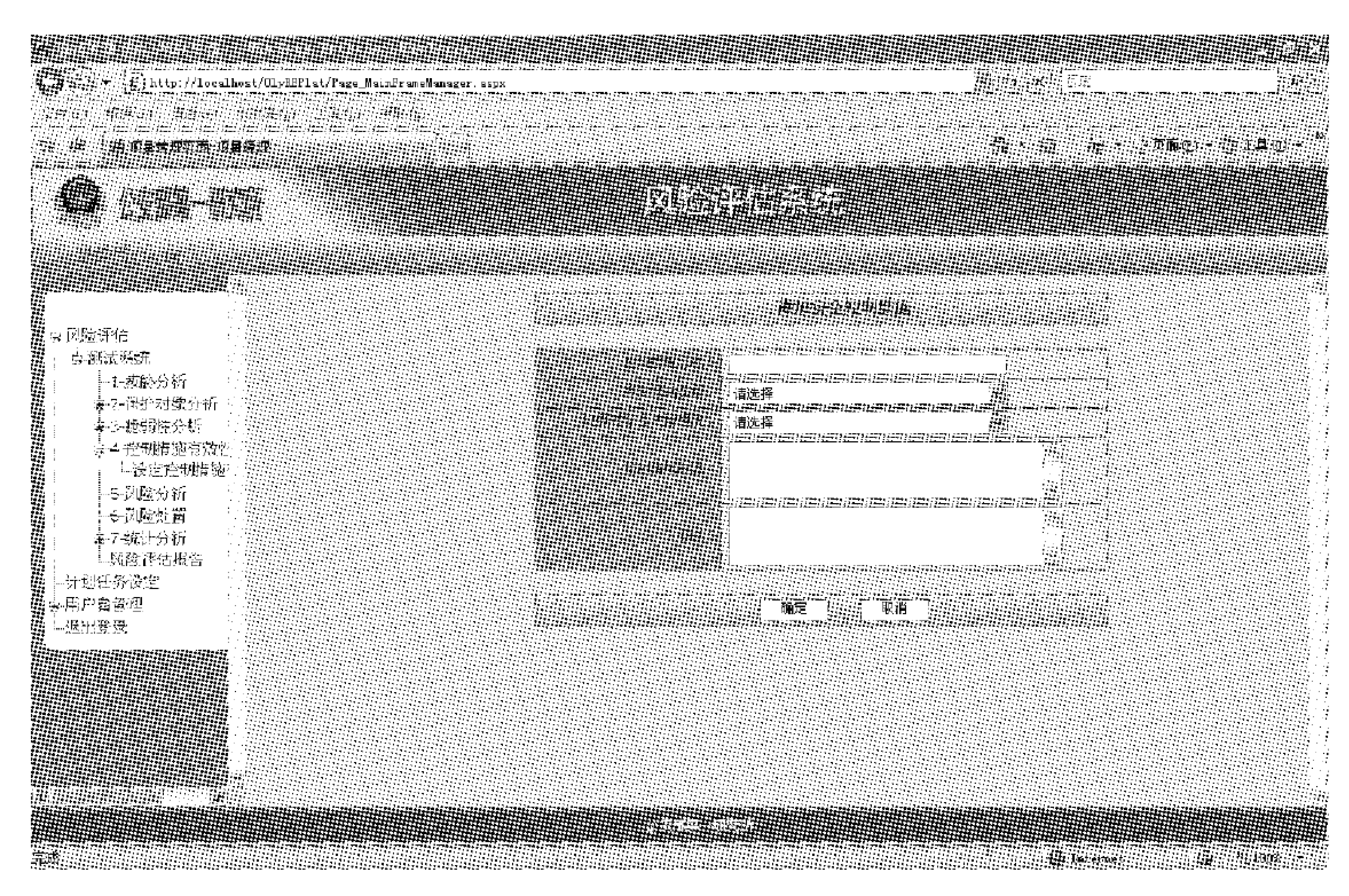



图 6-29　控制措施添加对话框




图 6-30　控制措施查看对话框

(4) 设定控制措施有效性等级

单击左侧"设定控制措施有效性等级"链接进入设置页面，如图 6-31 所示。

图 6-31 控制措施有效性等级设置页面

单击对应控制措施一栏的"单击查看"链接，进入针对保护对象威胁的对应控制措施查看设置页面。在此页面可以设置哪些控制措施是针对此威胁的。选择欲选取的控制措施，单击"保存"按钮完成关联。单击控制措施名称可以在弹出窗口中查看控制措施的具体内容。

控制措施有效性分析页面右侧的下拉列表用来设置有效性等级，参考了相关联的控制措施后，在这里设定一个综合的等级。选择完毕后单击"保存本页"按钮可完成保存。单击"保存全部"按钮可保存所有针对威胁的有效性等级，但是其他页面的等级会以"很低"保存。

### 6. 风险分析

单击左侧"风险分析"链接进入风险分析页面，如图 6-32 所示。单击"计算风险"按钮可以重新计算风险值。

### 7. 风险处置

单击左侧"风险处置"链接，进入风险处置页面，如图 6-33 所示。此页面显示等级为高或者极高的风险。可单击左侧树进行分类查看。单击具体威胁的"查看详情"进入查看页面。单击"修改"按钮，进入修改对话框对风险处置的相应信息进行修改。

### 8. 统计分析

展开左侧"统计分析"选项，会看到四个子项目：保护对象统计、威胁统计、脆弱性统计和风险统计。保护对象统计针对保护对象的重要性等级进行统计，威胁统计针对威胁的威胁等级进行统计，脆弱性统计针对脆弱性的脆弱性等级进行分析，风险统计针对保护对象的风险等级进行统计。这四项操作基本相同，现仅介绍保护对象统计。

图 6-32 风险分析页面




图 6-33 风险处置页面

保护对象统计页面如图 6-34 所示。图形左上选择统计图或者分布图，下面的列表选择保护对象的类型。统计图最多显示 10 个，如果超过 10 个可以单击图形下方链接查看所有统计图。如图 6-35 和图 6-36 所示。



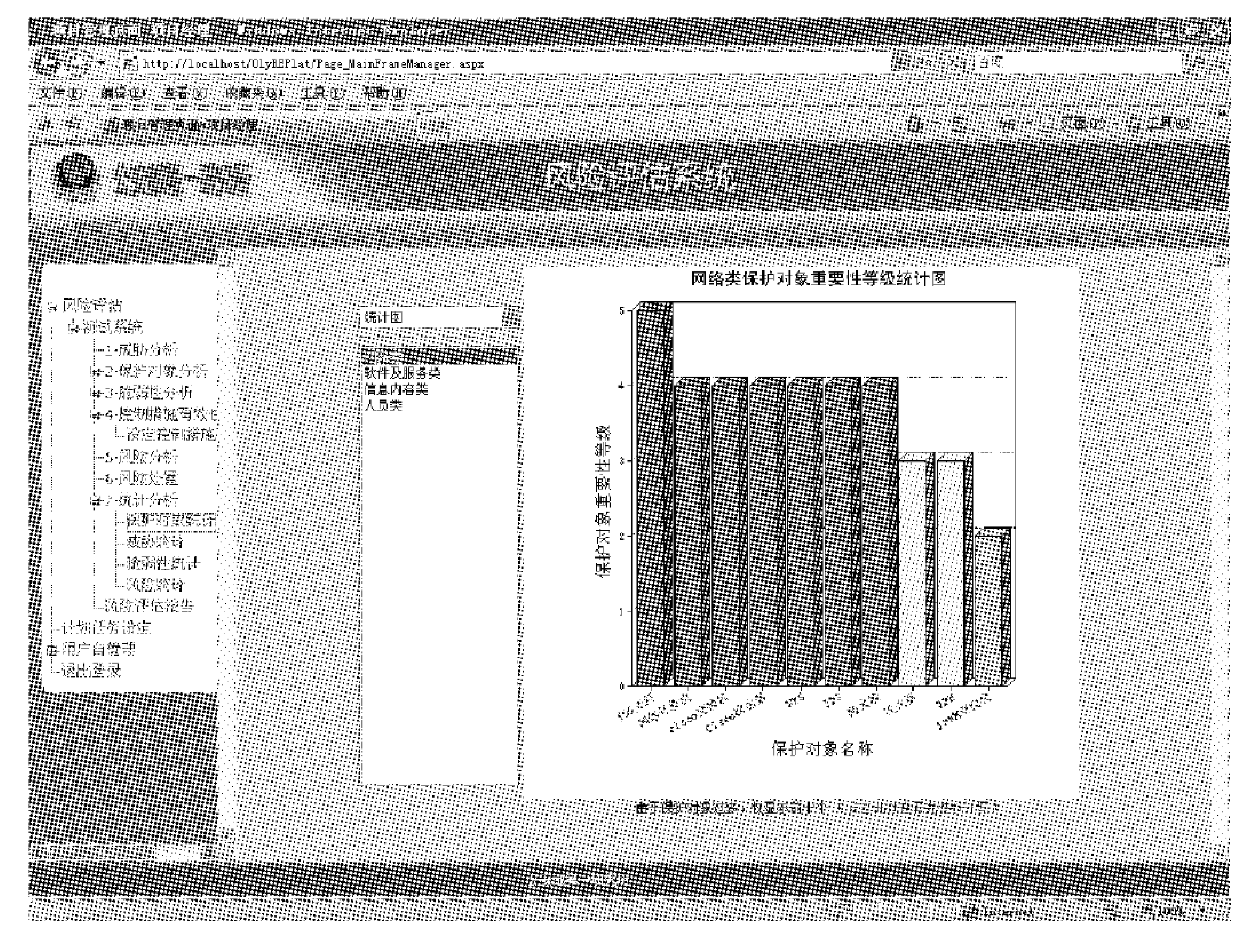



图 6-34 统计图

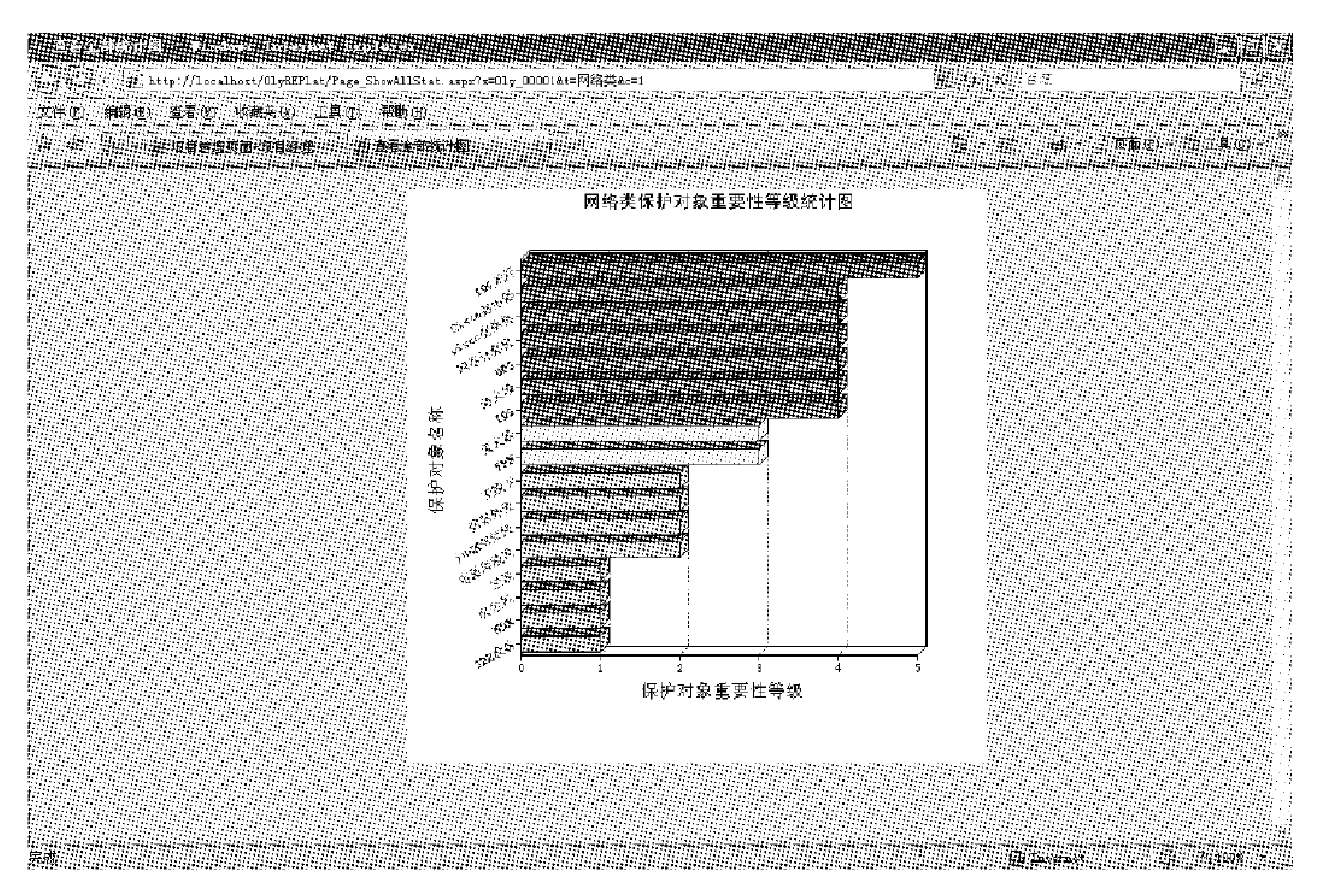



图 6-35 全部统计图

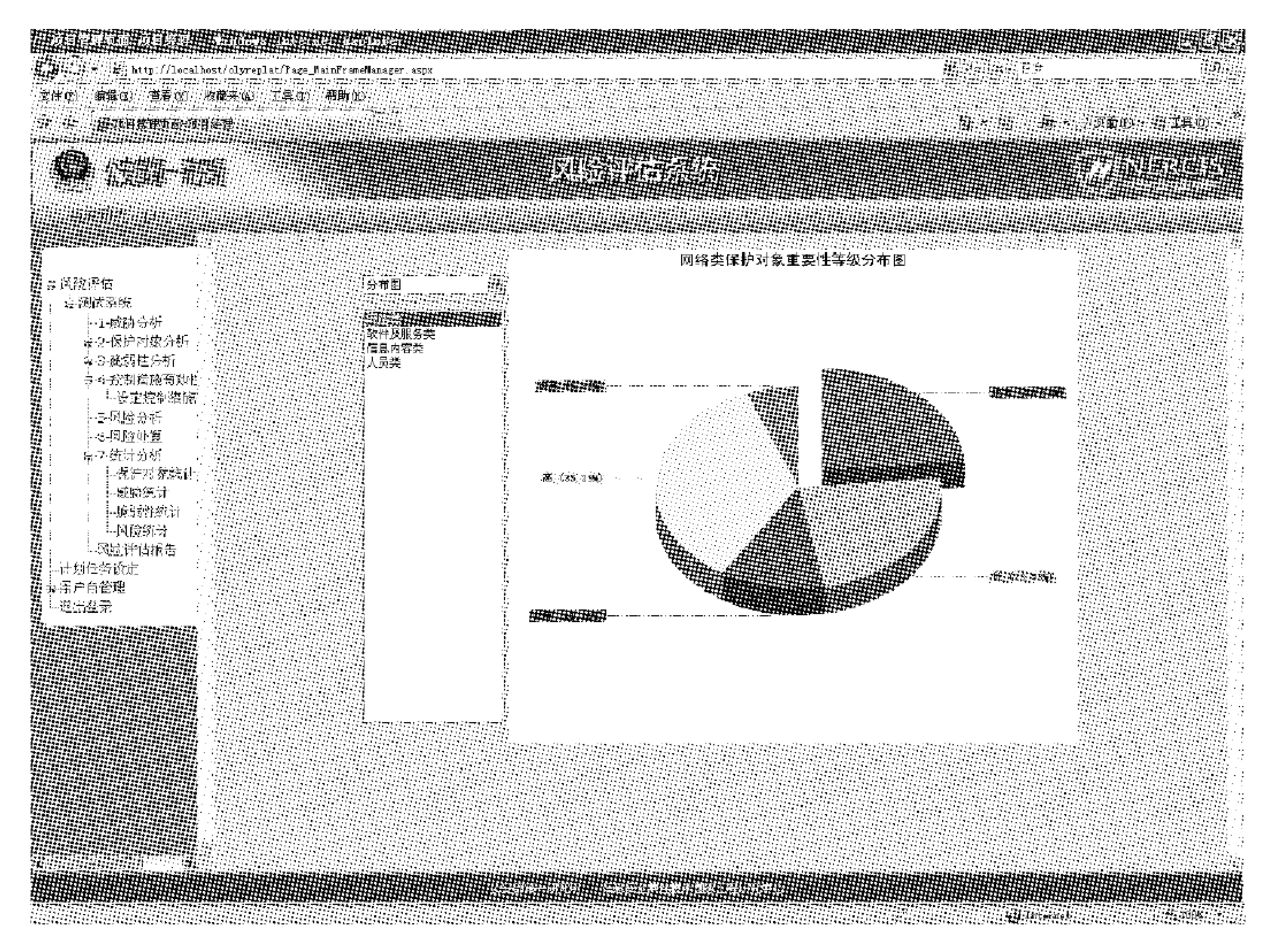



图 6-36 分布图

## 9. 评估报告生成

单击左侧“风险评估报告”链接，进入评估报告生成对话框，如图 6-37 所示。单击“向

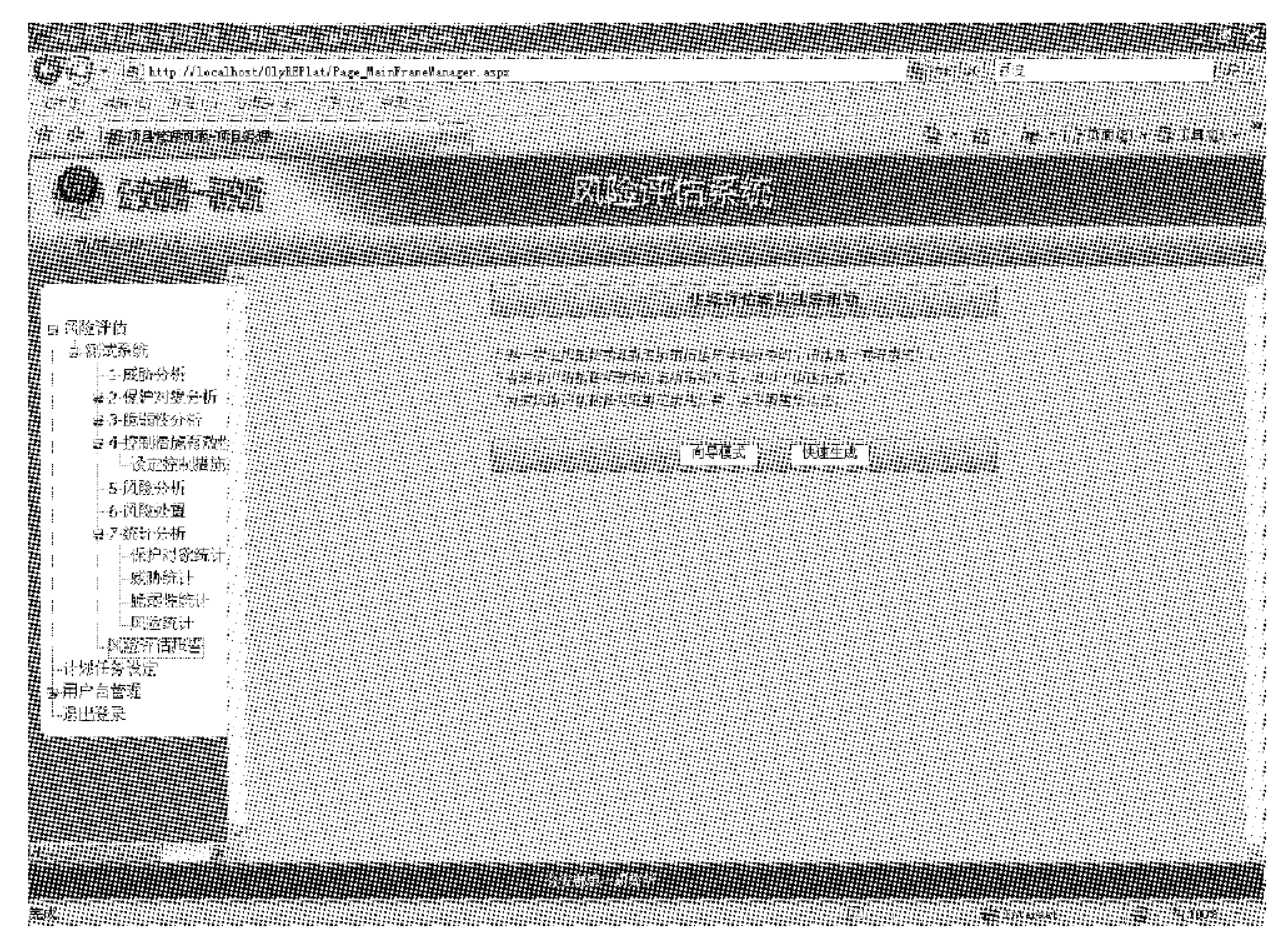



图 6-37 评估报告生成对话框

导模式"按钮进入报告参数设定。分别需要设定风险评估报告的目的和意义、风险评估的依据、风险评估的责任单位和信息网络安全的风险等级四个内容。设定完成后单击"快速生成"按钮，稍待片刻即可生成评估报告，如图 6-38 所示。注意，生成评估报告时会杀死存在的 Word 进程，因此生成前请保存并关闭打开的 Word 文档。

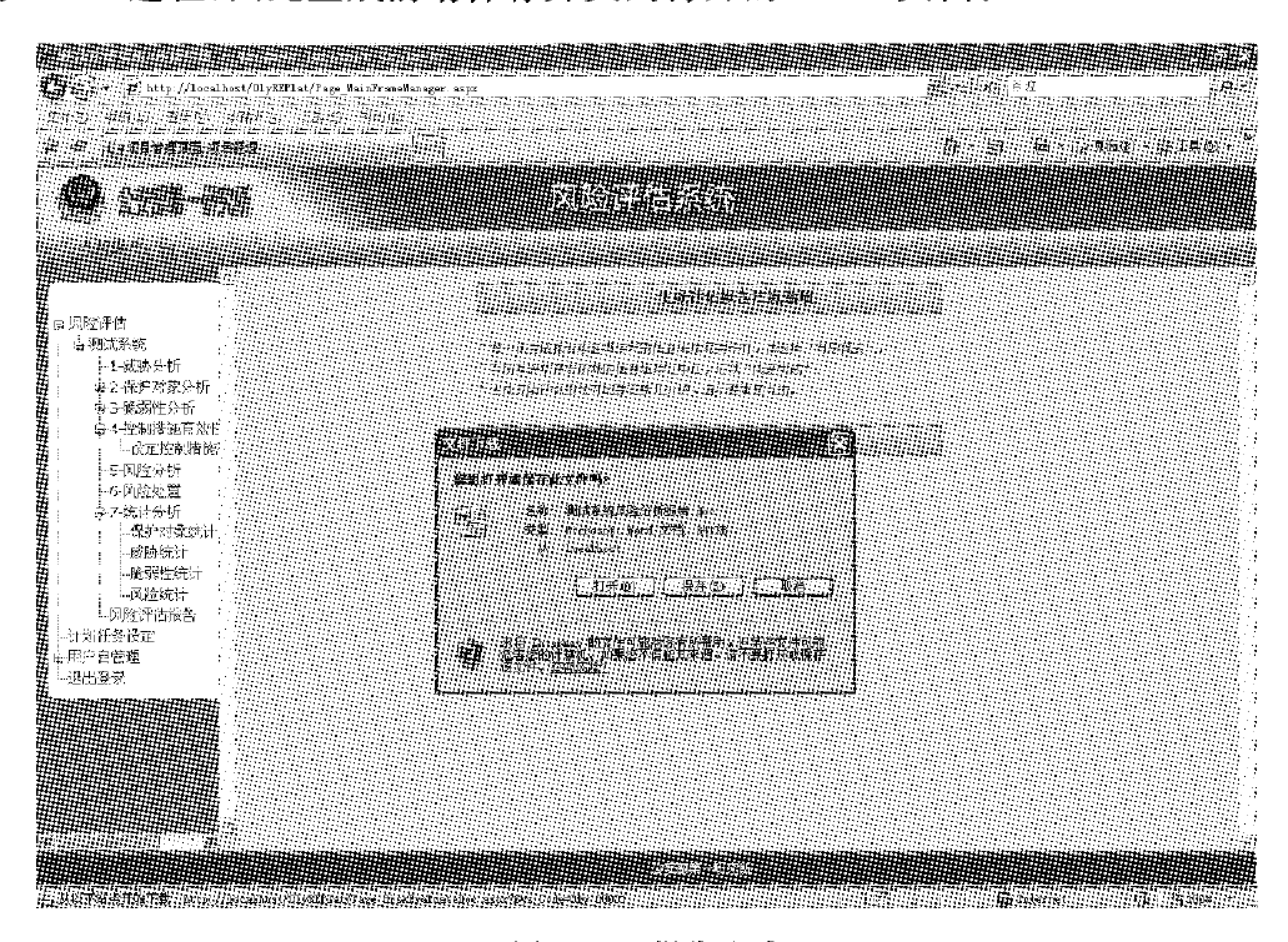



图 6-38 报告生成

### 10. 计划任务设定

单击左侧"计划任务设定"链接可进入计划任务对话框，如图 6-39 所示。在此对话框单击下拉列表选择欲设定的项目。然后为每一步骤选择计划结束时间，单击"确定"按钮进行保存。还可以通过单击"建议计划安排"按钮进行默认设定。默认设定为每一个步骤耗时五天。

## 6.4.4 技术测试人员操作指南

技术测试人员负责脆弱性扫描结果的导入。

## 6.4.5 管理核查人员操作指南

管理核查人员负责管理核查问卷的生成。登录后依次展开左侧列表，单击"生成问卷"按钮，进入问卷生成对话框，如图 6-40 所示。如果没有问卷，可以单击"生成问卷"按钮，进入生成对话框，如图 6-41 所示。在左侧选择待生成的问题类别，单击"确定生成"按钮即可。

如果问卷评估页面中显示的是现在系统中已经生成的问卷，则可以通过上方的下拉列表进行过滤，便于一类类地查看。如果想要重新生成，单击"重新生成"按钮，进入重新生成对话框。

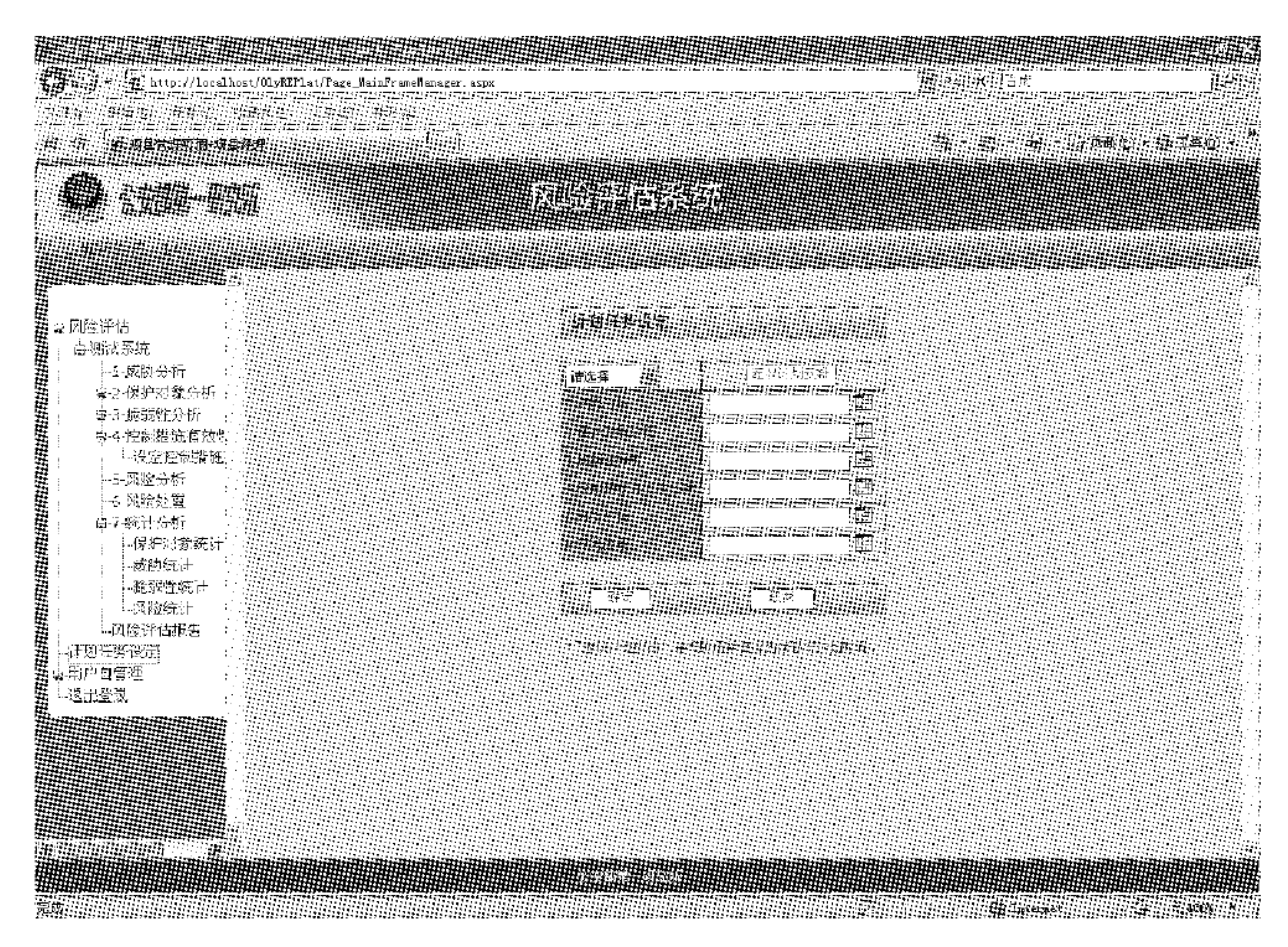


图 6-39 计划任务设定对话框



图 6-40 问卷生成对话框



图 6-41　生成对话框

## 6.4.6　手工检查人员操作指南

手工检查人员按照测试表单对项目进行手工检查。

# 参考文献

[1] 《信息系统等级保护安全设计技术要求》(GB/T 24856—2009),2009.

[2] 中华人民共和国国家标准.计算机信息系统安全保护等级划分准则(GB 17859—1999),1999.

[3] 公安部,国家保密局,国家密码管理局,等.信息安全等级保护管理办法.公通字[2007] 43号文件.

[4] 中华人民共和国国家标准.信息安全技术 信息安全风险评估规范(GB/T 20984—2007),2007.

[5] 范红,厉剑,胡志昂,等.对《国际信息系统等级保护安全设计技术要求》的认识与研究.全国计算机安全学术交流会论文集,2009.

[6] 范红.信息安全风险评估规范国家标准理解与实施.北京:中国标准出版社,2007.

[7] 范红,冯登国.信息安全风险评估实施教程.北京:清华大学出版社,2007.

[8] 范红,等.信息安全风险评估方法与应用.北京:清华大学出版社,2006.

[9] 范红.国家信息安全风险评估标准的研究与探讨.中国信息协会信息安全专业委员会年会论文集,2005.

[10] 金丽娜,等.高端防火墙中包分类的实现研究.全国计算机安全学术交流会论文集,2009.

[11] Commission of the European Communities. Information Technology Security Evaluation Criteria (ITSEC). Version 1.2.1991.

[12] NIST. Risk Management Guide for Information Technology Systems. NIST-SP-800-30.2001.

[13] National Security Agency. Information Assurance Technical Framework(IATF), Version 3.0.2000,http://www.iatf.net.

# 读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。


地址：北京市海淀区双清路学研大厦 A 座 602 室 计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544


教材名称：信息系统等级保护安全设计技术实现与使用

ISBN：978-7-302-21795-4

**个人资料**

姓名：________ 年龄：____ 所在院校/专业：__________

文化程度：________ 通信地址：______________

联系电话：________ 电子信箱：______________

**您使用本书是作为：** □指定教材 □选用教材 □辅导教材 □自学教材

**您对本书封面设计的满意度：**

□很满意 □满意 □一般 □不满意　改进建议__________

**您对本书印刷质量的满意度：**

□很满意 □满意 □一般 □不满意　改进建议__________

**您对本书的总体满意度：**

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

**本书最令您满意的是：**

□指导明确 □内容充实 □讲解详尽 □实例丰富

**您认为本书在哪些地方应进行修改？（可附页）**

______________________________

______________________________

**您希望本书在哪些方面应进行改进？（可附页）**

______________________________

______________________________

# 电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。